myessentials

Wireless G Router

User Manual

ME1004-R

Table of Contents

1. Introduction 1
Benefits of a Home Network 1
Advantages of a Wireless Network 1
Placement of your Router for Optimal Performance 2
2. Product Overview 6
Product Features 6
3. Knowing your Router 9
Package Contents 9
System Requirements 9
Quick Installation Software System Requirements 9
4. Connecting and Configuring your Router 14
5. Alternate Setup Method 22
6. Using the Web-Based Advanced User Interface 25
Changing LAN Settings 36
Viewing the DHCP Client List Page 38
Configuring the Wireless Network Settings 39
Securing your Wi-Fi Network 44
WEP Setup 49
WPA Setup 51
Setting WPA/WPA2 51
Guest Access (Optional) 52
Using the Access Point Mode 55
Configuring the Firewall 56
Setting MAC Address Filtering 59
Enabling the DMZ 60
Utilities Tab 62
Restarting the Router 63
Updating the Firmware 67
7. Manually Configuring Network Settings 71
8. Recommended Web Browser Settings 76
9. Troubleshooting 78
10. Information 92

Introduction

Thank you for purchasing the Wireless G Router (the Router) from MyEssentials. The following two short sections discuss the benefits of home networking and outline best practices for maximizing your wireless home network range and performance. Please be sure to read through this User Manual completely, and pay special attention to the section entitled "Placement of your Router for Optimal Performance" on page 2.

Benefits of a Home Network

- Share one high-speed Internet connection with all the computers in your home
- Share resources, such as files, and hard drives among all the connected computers in your home
- Share a single printer with the entire family
- Share documents, music, video, and digital pictures
- Store, retrieve, and copy files from one computer to another
- Simultaneously play games online, check Internet email, and chat

Advantages of a Wireless Network

- **Mobility** – you'll no longer need a dedicated "computer room" —now you can work on a networked laptop or desktop computer anywhere within your wireless range
- **Easy installation** – The MyEssentials Quick Installation Software makes setup simple
- **Flexibility** – set up and access printers, computers, and other networking devices from anywhere in your home
- **Easy expansion** – the wide range of MyEssentials networking products lets you expand your network to include devices such as printers and gaming consoles
- **No cabling required** – you can spare the expense and hassle of retrofitting Ethernet cabling throughout the home or office
- **Widespread industry acceptance** – choose from a wide range of interoperable networking products

Placement of your Router for Optimal Performance

Important Factors for Placement and Setup

Your wireless connection will be stronger the closer your computer is to your Router. Typical indoor operating range for wireless devices is between 100 and 200 feet.

In the same way, your wireless connection and performance will degrade somewhat as the distance between your Router and connected devices increases. This may or may not be noticeable to you. As you move farther from your Router, connection speed may decrease. Factors that can weaken signals simply by getting in the way of your network's radio waves are metal appliances or obstructions, and walls.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between five and 10 feet away from the Router in order to see if distance is the problem. If difficulties persist even at close range, please contact MyEssentials Technical Support:
US: 1-866-761-4608

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

1. Wireless Router Placement

Place your Router, the central connection point of your network, as close as possible to the center of your wireless network devices.

To achieve the best wireless network coverage for your "wireless clients" (i.e., computers enabled by Wireless Notebook Network Cards and Wireless USB Adapters from MyEssentials):

- Ensure that your Router's networking antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your Router itself is positioned vertically, point the antennas as much as possible in an upward direction.
- In multistory homes, place the Router on a floor that is as close to the center of the home as possible. This may mean placing the Router on an upper floor.
- Try not to place the Router near a cordless phone.

2. Avoid Obstacles and Interference

Avoid placing your Router near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path (between your computers and Router).

3. Cordless Phones

If the performance of your wireless network is impaired after attending to the above issues, and you have a cordless phone:

- Try moving cordless phones away from the Router and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check the manufacturer's information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Router to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz cordless phone.

4. Choose the "Quietest" Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with yours.

Use the Site Survey capabilities found in the wireless utility of your wireless adapter or card to locate any other wireless networks that are available (see your wireless adapter's or card's user manual), and move your Router and computers to a channel as far away from other networks as possible.

- Experiment with more than one of the available channels in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.
- For wireless networking products from MyEssentials, use the detailed Site Survey and wireless channel information included with your Wireless Network Card or Adapter. See your Network Card's user guide for more information.

5. Secure Connections, VPNs, and AOL

Secure connections typically require a user name and password, and are used where security is important. Secure connections include:

- Virtual Private Network (VPN) connections, often used to connect remotely to an office network
- The "Bring Your Own Access" program from America Online (AOL), which lets you use AOL through broadband provided by another DSL or cable service
- Most online banking websites
- Many commercial websites that require a user name and password to access your account

Secure connections can be interrupted by a computer's power management setting, which causes it to "go to sleep." The easiest solution to avoid this is to simply reconnect by rerunning the VPN or AOL software, or by re-logging into the secure website.

A second alternative is to change your computer's power management settings so it does not go to sleep; however, this may not be appropriate for portable computers. To change your power management setting under Windows, see the "Power Options" item in the Control Panel.

If you continue to have difficulty with secure connections, VPNs, and AOL, please review the steps above to be sure you have addressed these issues.

For more information regarding our networking products, visit our website at **www.MyEssentialssupport.com** or call MyEssentials Technical Support at:

US: 1-866-761-4608

Product Overview

Product Features

In minutes you will be able to share your Internet connection and network your computers. The following is a list of features that make your new Wireless G Router from MyEssentials an ideal solution for your home or small office network.

Works with Both PCs and Mac® Computers

The Router supports a variety of networking environments including Mac OS®, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 98, Me, NT®, 2000, and XP, and others. All that is needed is an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

Front-Panel LED Display

Lighted LEDs on the front of the Router indicate which functions are in operation. You'll know at-a-glance whether your Router is connected to the Internet. This feature eliminates the need for advanced software and status-monitoring procedures.

Web-Based Advanced User Interface

You can set up the Router's advanced functions easily through your web browser, without having to install additional software onto the computer. There are no disks to install or keep track of and, best of all, you can make changes and perform setup functions from any computer on the network quickly and easily.

NAT IP Address Sharing

Your Router employs Network Address Translation (NAT) to share the single IP address assigned to you by your Internet Service Provider while saving the cost of adding IP addresses to your Internet service account.

SPI Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect, and fragment flooding.

Integrated 10/100 4-Port Switch

The Router has a built-in, 4-port network switch to allow your wired computers to share printers, data and MP3 files, digital photos, and much more. The switch features automatic detection so it will adjust to the speed of connected devices. The switch will transfer data between computers and the Internet simultaneously without interrupting or consuming resources.

Universal Plug-and-Play (UPnP) Compatibility

UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant.

Support for VPN Pass-Through

If you connect to your office network from home using a VPN connection, your Router will allow your VPN-equipped computer to pass through the Router and to your office network.

Built-In Dynamic Host Configuration Protocol (DHCP)

Built-In Dynamic Host Configuration Protocol (DHCP) on-board makes for the easiest possible connection of a network. The DHCP server will assign IP addresses to each computer automatically so there is no need for a complicated networking setup.

Quick Installation Software

The Quick Installation Software takes the guesswork out of setting up your Router. This automatic software determines your network settings for you and sets up the Router for connection to your Internet Service Provider (ISP). In a matter of minutes, your Wireless Router will be up and running on the Internet.

NOTE: Quick Installation Software is compatible with Windows 98SE, Me, 2000, XP, and Mac OS X. If you are using another operating system, the Wireless Router can be set up using the Alternate Setup Method described in this User Manual (see page 22).

Integrated 802.11g Wireless Access Point

802.11g is an exciting new wireless technology that achieves data rates up to 54Mbps, nearly five times faster than 802.11b.

MAC Address Filtering

For added security, you can set up a list of MAC addresses (unique client identifiers) that are allowed access to your network. Every computer has its own MAC address. Simply enter these MAC addresses into a list using the Web-Based Advanced User Interface and you can control access to your network.

Knowing your Router

Package Contents

- Wireless G Router
- Quick Installation Guide
- MyEssentials Quick Installation Software CD with User Manual
- MyEssentials RJ45 Ethernet Networking Cable
- Power Supply

System Requirements

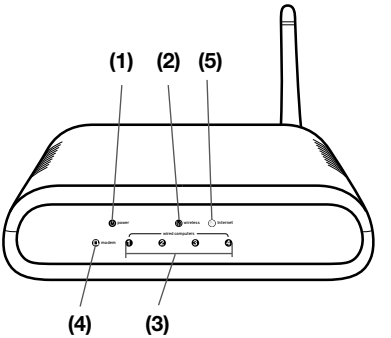
- Broadband Internet connection such as a DSL or cable modem with RJ45 (Ethernet) connection
- At least one computer with an installed network interface adapter
- TCP/IP networking protocol installed on each computer
- RJ45 Ethernet networking cable
- Internet browser

Quick Installation Software System Requirements

- A PC running Windows 98SE, Me, 2000, or XP, or a Mac computer running Mac OS X
- Minimum 64MB RAM
- Internet browser

Knowing your Router

The Router has been designed to be placed on a desktop. All of the cables exit from the rear of the Router for better organization and utility. The LED indicators are easily visible on the front of the Router to provide you with information about network activity and status.



1. ⏻

When you apply power to the Router or restart it, a short period of time elapses while the Router boots up. During this time, the Power/Ready LED blinks. When the Router has completely booted up, the Power/Ready LED becomes a SOLID light, indicating the Router is ready for use.

OFF	Router is OFF
Blinking Green	Router is Booting Up
Solid Green	Router is Ready

2. (ᵛ)

OFF	Wireless Network is OFF
Green	Wireless Network is Ready
Blinking	Indicates Wireless Activity

3. 1 2 3 4

These LEDs are labeled 1–4 and correspond to the numbered ports on the rear of the Router. When a computer is properly connected to one of the wired computer ports on the rear of the Router, the LED will light. GREEN means a 10Base-T device is connected, AMBER means a 100Base-T device is connected. When information is being sent over the port, the LED blinks rapidly.

OFF	No Device is Linked to the Port
Green	10/100Base-T Device Connected
Blinking (Orange or Green)	Port Activity

4.

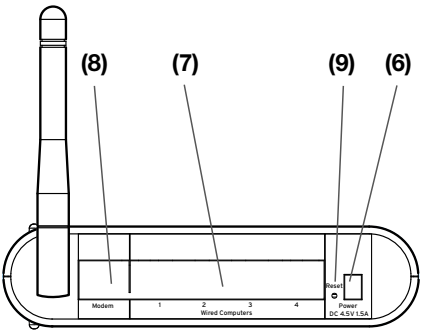
This LED lights in GREEN to indicate that your modem is connected properly to the Router. It blinks rapidly when information is being sent over the port between the Router and the modem.

OFF	No WAN Link
Solid Green	Good WAN Link
Blinking Green	WAN Activity

5.

This unique LED shows you when the Router is connected to the Internet. When the light is OFF, the Router is NOT connected to the Internet. When the light is blinking, the Router is attempting to connect to the Internet. When the light is solid GREEN, the Router is connected to the Internet. When using the “Disconnect after x minutes” feature, this LED becomes extremely useful in monitoring the status of your Router’s connection.

OFF	Router is not Connected to the Internet
Blinking Green	Router is Attempting to Connect to the Internet
Solid Green	Router is Connected to the Internet



6. Power Jack

Connect the included 5V DC power supply to this jack.

7. Wired Computers

Connect your wired (non-wireless) computers to these ports. These ports are RJ45, 10/100 auto-negotiation, auto-uplinking ports for standard UTP category 5 or 6 Ethernet cable. The ports are labeled 1 through 4. These ports correspond to the numbered LEDs on the front of the Router.

8. Modem

This port is for connection to your DSL or cable modem. Use the cable that was provided with the modem to connect the modem to this port. Use of a cable other than the cable supplied with the cable modem may not work properly.

9. Reset

The "Reset" button is used in rare cases when the Router may function improperly. Resetting the Router will restore the Router's normal operation while maintaining the programmed settings. You can also restore the factory default settings by using the "Reset" button. Use the restore option in instances where you may have forgotten your custom password.

a. Resetting the Router

Push and release the "Reset" button. The lights on the Router will momentarily flash. The Power/Ready light will begin to blink. When the Power/Ready light becomes solid again, the reset is complete.

b. Restoring the Factory Defaults

Press and hold the "Reset" button for at least 10 seconds, then release it. The lights on the Router will momentarily flash. The "Power/Ready" light will begin to blink. When the "Power/Ready" light becomes solid again, the restore is complete.

Connecting and Configuring your Router

Verify the contents of your box. You should have the following:

- Wireless G Router
- Quick Installation Guide
- MyEssentials Quick Installation Software CD with User Manual
- RJ45 Ethernet Networking Cable (for connection of the Router to the computer)
- Power Supply

Modem Requirements

Your DSL or cable modem must be equipped with an RJ45 Ethernet port. Many modems have both an RJ45 Ethernet port and a USB connection. If you have a modem with both Ethernet and USB, and are using the USB connection at this time, you will be instructed to use the RJ45 Ethernet port during the installation procedure. If your modem has only a USB port, you can request a different type of modem from your ISP, or you can, in some cases, purchase a modem that has an RJ45 Ethernet port on it.

ALWAYS INSTALL YOUR ROUTER FIRST! IF YOU ARE INSTALLING NUMEROUS NETWORK DEVICES FOR THE FIRST TIME, IT IS IMPORTANT THAT YOUR ROUTER IS CONNECTED AND RUNNING BEFORE ATTEMPTING TO INSTALL OTHER NETWORK COMPONENTS SUCH AS NOTEBOOK CARDS AND DESKTOP CARDS.

Quick Installation Software

MyEssentials has provided our Quick Installation Software to make installing your Router a simple and easy task. You can use it to get your Router up and running in minutes.

The Quick Installation Software requires that your Windows 98SE, Me, 2000, XP, or Mac OS X v10.1.x computer be connected directly to your DSL or cable modem and that the Internet connection is active and working at the time of installation. If it is not, you must use the “Alternate Setup Method” section of this User Manual to configure your Router. Additionally, if you are using an operating system other than Windows 98SE, Me, 2000, or XP, you must set up the Router using the “Alternate Setup Method” section of this User Manual.

IMPORTANT: Run the Quick Installation Software from the computer that is directly connected to the DSL or cable modem. **DO NOT CONNECT THE ROUTER AT THIS TIME.**

Connecting and Configuring your Router

Step 1 | Run the Quick Installation Software

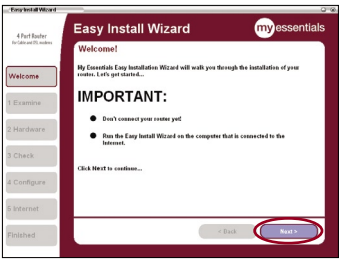
1.1 Shut down any programs that are running on your computer at this time.

1.2 Make sure you have the following items at the computer that is now directly connected to the DSL or cable modem. DO NOT CONNECT THE ROUTER AT THIS TIME.

- Quick Installation Guide
- The Quick Installation Software CD with User Manual
- The Router
- The Router's Power Supply
- RJ45 Ethernet Networking Cable

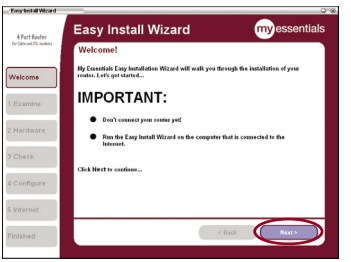
1.3 Turn off any firewall or Internet-connection-sharing software on your computer.

1.4 Insert the Quick Installation Software CD into your CD-ROM drive. The Easy Installation Wizard screen will automatically appear on your screen within 15 seconds. If it does not, select your CD-ROM drive from "My Computer" and double-click on the file named "EasyInstall.exe" on the CD-ROM.



Welcome Screen
After you insert the CD into your CD-ROM drive, the Wizard's welcome screen will appear. Make sure you have not connected the Router at this point. If you have connected your Router, please reconnect your computer directly to the modem. Click "Run the Quick Installation Software" when you are ready to move on.

Progress Screen
The Quick Installation Software will show you a progress screen each time a step in the setup has been completed. Each time you see the progress screen, click "Next" when you are ready to move to the next step.



Examining Settings
The Wizard will now examine your computer's network settings and gather information needed to complete the Router's connection to the Internet. When the Wizard is finished examining your computer, click "Next" to continue.

Multiple Network Adapters Found Screen
If you have more than one network adapter installed in your computer, this screen will appear. If you have more than one network adapter installed in your computer, the Wizard will need to know which adapter is connected to your modem. Select the network adapter that is connected to your modem from the list and click "Next". If you are not sure which adapter to choose, select the adapter at the top of the list. If you mistakenly choose the wrong adapter now, you will be able to choose a different one later.

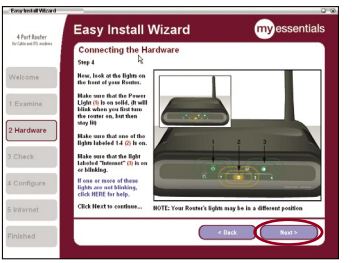
Step 2 | Set up the Hardware

The Wizard will walk you through connecting your Router to your computer and modem. Follow the steps on the screen using the pictures as a guide.

2.1 This step instructs you to locate the cable connected between your modem and the networking port on your computer. Unplug this cable from the computer and plug it into the GREEN port on the Router. Click “Next” to continue.

2.2 This step instructs you to locate the BLUE cable that is included with your Router. Plug one end of this cable into ANY one of the BLUE ports on your Router. Plug the other end of the cable into the networking port on your computer. Click “Next” to continue.

2.3 This step instructs you to locate the power supply that is included with your Router. Plug the power supply's small connector into the power port on the Router. Plug the power supply into an empty power outlet. Click "Next" to continue.


Easy Install Wizard
myessentials
Connecting the Hardware
Step 4
Now, look at the lights on the front of your Router.
Make sure that the Power Light is on solid. It will blink when you first turn the router on, but then stay lit.
Make sure that one of the lights labeled 1-4 is on.
Make sure that the light labeled "Internet" is on or blinking.
If one or more of these lights are not blinking, click HERE for help.
Click Next to continue...
NOTE: Your Router's lights may be in a different position
< Back
Next >
Welcome
1 Examine
2 Hardware
3 Check
4 Configure
5 Internet
Finished

2.4 This step instructs you to look at the lights on the front of your Router. Make sure the appropriate lights are ON. Refer to the Quick Installation Software on your computer's screen for more details. Click "Next" to continue. Note: The Quick Installation Software may ask you to reboot your computer. If it does, reboot your computer and proceed with the installation.

Step 3 | Check the Connection

3.1 Once you have completed connecting the Router, the Wizard will check the connection to the Router and then go on to determine what type of Internet connection you have.

3.2 User Name and Password Needed

If you have a connection type that requires a user name and a password, the Wizard will ask you to type in your user name and password. If your connection type does not require a user name and password, you will not see this screen.

Your user name and password is provided to you by your Internet Service Provider. If you have to type in a user name and password to connect to the Internet, then type that same user name and password in here. Your user name looks something like “jsmith@myisp.com” or simply “jsmith”. The service name is optional and is very rarely required by your ISP. If you don’t know your service name, leave this blank. When you have entered your information, click “Next” to move on.

3.3 Wireless Setup

This step is optional. Click “Next” if you want to skip it. Using this step, you can customize your wireless network settings if you want to. Follow the steps on the screen to complete this step. Click “Next” to continue.

Step 4 | Secure your Network

4.1 After connection has been established, you will be prompted by the Quick Installation Software to select your desired security level.

4.2 WEP and WPA are the two security options. If you do not want security or would prefer to install at a later time, click the radio button next to “NONE” and click “Next.”

4.3 The Wi-Fi Protected Access (WPA) security option features a two-password setup. You can select one password that provides COMPLETE NETWORK access and another password for GUEST (Internet only) access only. Click “Next”.

4.4 Security setup is now complete. Click “Next” to configure.

Step 5 | Configure the Router

The Wizard will now transfer all of the configuration information to the Router. This will take approximately one minute. During this time, do not turn off the Router or computer. The Router will restart itself at the end of this step.

5.1 Checking Internet

The Wizard will now check for an Internet connection. This can take a few minutes. The Wizard may not detect a connection right away. If not, it will retry a number of times. The “Connected” light on the front panel of the Router will flash during this time. Please be patient through this process.

5.2 Finished

When the Internet connection is complete, the Wizard will tell you that you are finished. The “Connected” LED on the front of the Router will be solid GREEN, indicating that the Router is now connected to the Internet.

Your Router is now connected to the Internet. Now you can begin surfing the Internet by opening your browser and going to your favorite web page.

Congratulations. You have finished installing your new MyEssentials Router. You are ready to set up the other computers in your home. You can also add computers to your Router anytime you want.

Alternate Setup Method

The Web-Based Advanced User Interface is a web-based tool that you can use to set up the Router if you don't want to use the Quick Installation Software. You can also use it to manage advanced functions of the Router. From the Web-Based Advanced User Interface, you can perform the following tasks:

- View the Router's current settings and status
- Configure the Router to connect to your ISP with the settings that they provided you
- Change the current network settings such as the Internal IP address, the IP address pool, DHCP settings, and more
- Set the Router's firewall to work with specific applications (port forwarding)
- Set up security features such as client restrictions, MAC address filtering, WEP, and WPA
- Enable the DMZ feature for a single computer on your network
- Change the Router's internal password
- Enable/Disable UPnP (Universal Plug-and-Play)
- Reset the Router
- Back up your configuration settings
- Reset the Router's default settings
- Update the Router's firmware

Alternate Setup Method

Step 1 | Connect your Router

1.1 Turn off the power to your modem by unplugging the power supply from the modem.

1.2 Locate the network cable that is connected between your modem and your computer and unplug it from your computer, leaving the other end connected to your modem.

1.3 Plug the loose end of the cable you just unplugged into the port on the back of the Router labeled “Modem”.

1.4 Connect a new network cable (not included) from the back of the computer to one of the wired computer ports labeled “1–4”.
Note: It does not matter which numbered port you choose.

1.5 Turn your DSL or cable modem on by reconnecting the power supply to the modem.

1.6 Before plugging the power cord into the Router, plug the cord into the wall, then plug the cord into the Router’s power jack.

1.7 Verify that your modem is connected to the Router by checking the lights on the front of the Router. The green light labeled “Modem” should be ON if your modem is connected correctly to the Router. If it is not, recheck your connections.

1.8 Verify that your computer is connected properly to the Router by checking the lights labeled “1–4”. The light that corresponds to the numbered port connected to your computer should be ON if your computer is connected properly. If it is not, recheck your connections.

Step 2 | Set up your Computer’s Network Settings to Work with a DHCP Server

See the section in this User Manual called “Manually Configuring Network Settings” for directions.

Step 3 Configure the Router Using the Web-Based Advanced User Interface

Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (you do not need to type in anything else such as "http://" or "www"). Then press the "Enter" key.

PLEASE NOTE: If you have difficulty accessing the Router's Web-Based Advanced User Interface, go to the section entitled "Manually Configuring Network Settings".

Logging into the Router

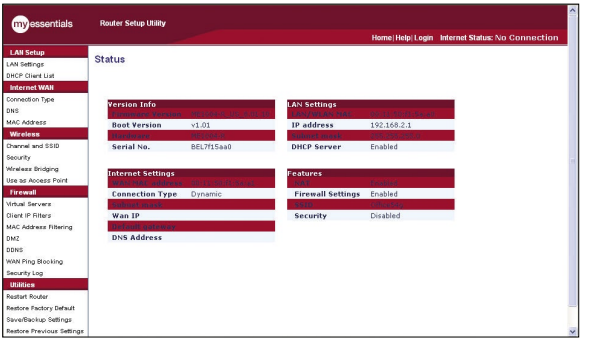
You will see the Router's home page in your browser window. The home page is visible to any user who wants to see it. To make any changes to the Router's settings, you have to log in. Clicking the "Login" button or clicking on any one of the links on the home page will take you to the login screen. The Router ships with no password entered. In the login screen, leave the password blank and click the "Submit" button to log in.

Logging out of the Router

One computer at a time can log into the Router for the purposes of making changes to the settings of the Router. Once a user has logged in to make changes, there are two ways that the computer can be logged out. Clicking the "Logout" button will log the computer out. The second method is automatic. The login will time out after a specified period of time. The default login time-out is 10 minutes. This can be changed from 1 to 99 minutes. For more information, see the section in this manual entitled "Changing the Login Time-Out Setting".

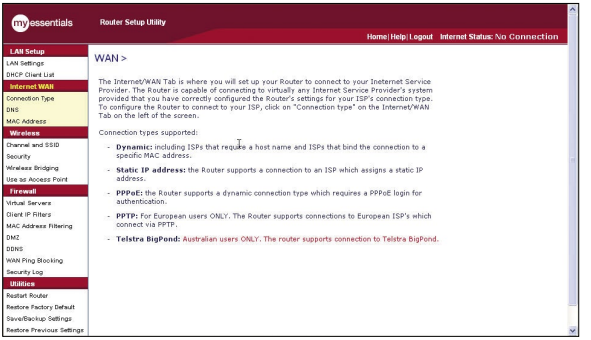
Using the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Web-Based Advanced User Interface (UI). The home page shows you a quick view of the Router's status and settings. All advanced setup pages can be reached from this page.



1. Quick-Navigation Links

You can go directly to any of the Router's UI pages by clicking directly on these links. The links are divided into logical categories and grouped by tabs to make finding a particular setting easier to find. Clicking on the purple header of each tab will show you a short description of the tab's function.


myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
WAN >
The Internet/WAN Tab is where you will set up your Router to connect to your Ineternet Service Provider. The Router is capable of connecting to virtually any Internet Service Provider's system provided that you have correctly configured the Router's settings for your ISP's connection type. To configure the Router to connect to your ISP, click on "Connection type" on the Internet/WAN Tab on the left of the screen.
Connection types supported:
- Dynamic: including ISPs that require a host name and ISPs that bind the connection to a specific MAC address.
- Static IP address: the Router supports a connection to an ISP which assigns a static IP address.
- PPPoE: the Router supports a dynamic connection type which requires a PPPoE login for authentication.
- PPTP: For European users ONLY. The Router supports connections to European ISP's which connect via PPTP.
- Telstra BigPond: Australian users ONLY. The router supports connection to Telstra BigPond.

2. Home Button

The "Home" button is available in every page of the UI. Pressing this button will take you back to the home page.

3. Internet Status Indicator

This indicator is visible in all pages of the UI, indicating the connection status of the Router. When the indicator says “connection OK” in GREEN, the Router is connected to the Internet. When the Router is not connected to the Internet, the indicator will read “no connection” in RED. The indicator is automatically updated when you make changes to the settings of the Router.

4. Login/Logout Button

This button enables you to log in and out of the Router with the press of one button. When you are logged into the Router, this button will change to read “Logout”. Logging into the Router will take you to a separate login page where you will need to enter a password. When you are logged into the Router, you can make changes to the settings. When you are finished making changes, you can log out of the Router by clicking the “Logout” button. For more information about logging into the Router, see the section called “Logging into the Router”.

5. Help Button

The “Help” button gives you access to the Router’s help pages. Help is also available on many pages by clicking “more info” next to certain sections of each page.

6. LAN Settings

Shows you the settings of the Local Area Network (LAN) side of the Router. Changes can be made to the settings by clicking on any one of the links (IP Address, Subnet Mask, DHCP Server) or by clicking the “LAN” “Quick Navigation” link on the left side of the screen.

7. Features

Shows the status of the Router’s NAT, firewall, and wireless features. Changes can be made to the settings by clicking on any one of the links or by clicking the “Quick Navigation” links on the left side of the screen.

8. Internet Settings

Shows the settings of the Internet/WAN side of the Router that connects to the Internet. Changes to any of these settings can be made by clicking on the links or by clicking on the “Internet/WAN” “Quick Navigation” link on the left side of the screen.

9. Version Info

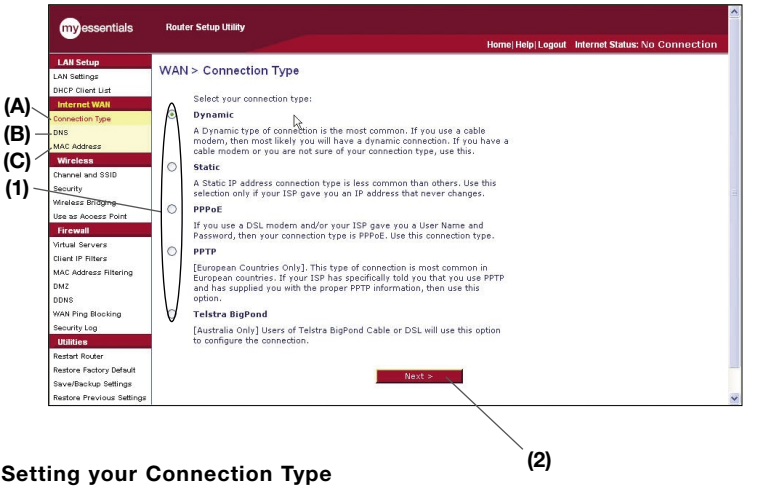
Shows the firmware version, boot-code version, hardware version, and serial number of the Router.

10. Page Name

The page you are on can be identified by this name. This User Manual will sometimes refer to pages by name. For instance “LAN > LAN Settings” refers to the “LAN Settings” page.

Step 4 Configure your Router for Connection to your Internet Service Provider (ISP)

The “Internet/WAN” tab is where you will set up your Router to connect to your Internet Service Provider (ISP). The Router is capable of connecting to virtually any ISP’s system provided you have correctly configured the Router’s settings for your ISP’s connection type. Your ISP connection settings are provided to you by your ISP. To configure the Router with the settings that your ISP gave you, click “Connection Type” **(A)** on the left side of the screen. Select the connection type you use. If your ISP gave you DNS settings, clicking “DNS” **(B)** allows you to enter DNS address entries for ISPs that require specific settings. Clicking “MAC address” **(C)** will let you clone your computer’s MAC address or type in a specific WAN MAC address, if required by your ISP. When you have finished making settings, the “Internet Status” indicator will read “connection OK” if your Router is set up properly.

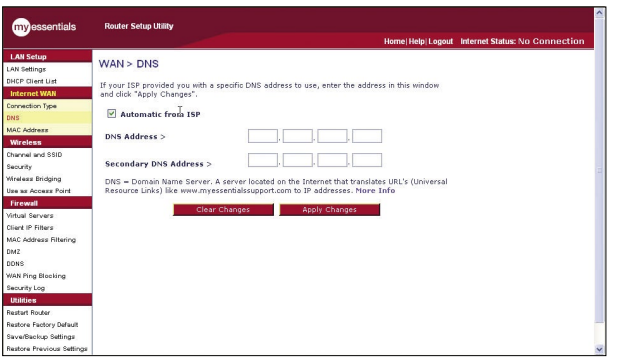

(A)
(B)
(C)
(1)
(2)
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
WAN > Connection Type
Select your connection type:
Dynamic
A Dynamic type of connection is the most common. If you use a cable modem, then most likely you will have a dynamic connection. If you have a cable modem or you are not sure of your connection type, use this.
Static
A Static IP address connection type is less common than others. Use this selection only if your ISP gave you an IP address that never changes.
PPPoE
If you use a DSL modem and/or your ISP gave you a User Name and Password, then your connection type is PPPoE. Use this connection type.
PPTP
[European Countries Only]. This type of connection is most common in European countries. If your ISP has specifically told you that you use PPTP and has supplied you with the proper PPTP information, then use this option.
Telstra BigPond
[Australia Only] Users of Telstra BigPond Cable or DSL will use this option to configure the connection.
Next >

Setting your Connection Type

From the “Connection Type” page, you can select the type of connection you use. Select the type of connection you use by clicking the button **(1)** next to your connection type and then clicking “Next” **(2)**.

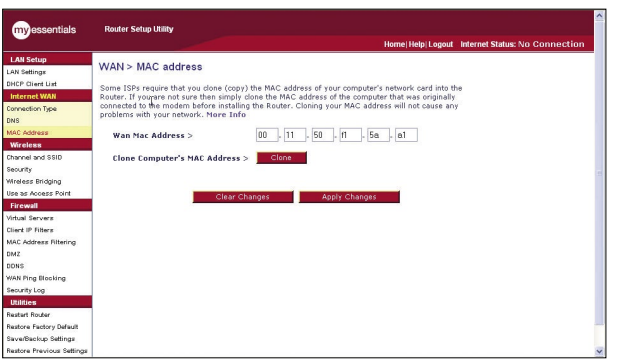
Setting your Internet Service Provider (ISP) Connection Type to Dynamic IP

A dynamic connection type is the most common connection type used with cable modems. Setting the connection type to “dynamic” in many cases is enough to complete the connection to your ISP. Some dynamic connection types may require a host name. You can enter your host name in the space provided if you were assigned one. Your host name is assigned by your ISP. Some dynamic connections may require that you clone the MAC address of the PC that was originally connected to the modem.



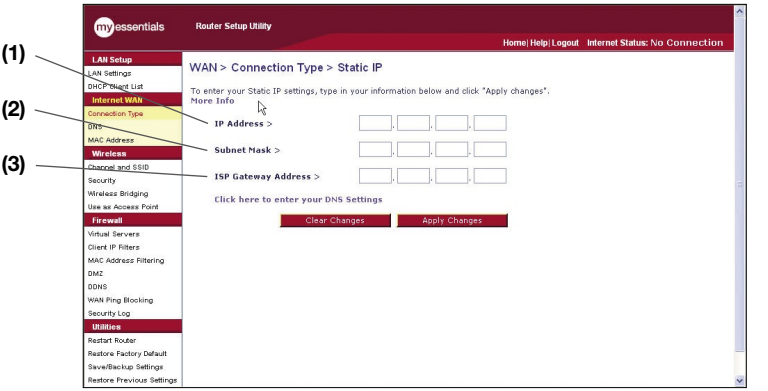
Change WAN MAC Address

If your ISP requires a specific MAC address to connect to the service, you can enter a specific MAC address or clone the current computer’s MAC address through this link.


myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
WAN > MAC address
Some ISPs require that you clone (copy) the MAC address of your computer's network card into the Router. If you are not sure then simply clone the MAC address of the computer that was originally connected to the modem before installing the Router. Cloning your MAC address will not cause any problems with your network. More Info
Wan Mac Address >
00 11 50 f1 5a a1
Clone Computer's MAC Address >
Clone
Clear Changes
Apply Changes

Setting your Internet Service Provider (ISP) Connection Type to Static IP

A static IP address connection type is less common than other connection types. If your ISP uses static IP addressing, you will need your IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you. Type in your information, then click “Apply Changes” **(5)**. After you apply the changes, the “Internet Status” indicator will read “connection OK” if your Router is set up properly.



1. IP Address

Provided by your ISP. Enter your IP address here.

2. Subnet Mask

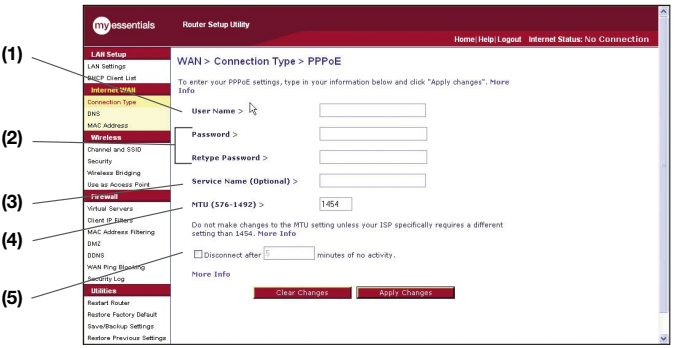
Provided by your ISP. Enter your subnet mask here.

3. ISP Gateway Address

Provided by your ISP. Enter the ISP gateway address here.

Setting your ISP Connection Type to PPPoE

Most DSL providers use PPPoE as the connection type. If you use a DSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service. If you have an Internet connection in your home or small office that doesn't require a modem, you may also use PPPoE.



Your connection type is PPPoE if:

1) Your ISP gave you a user name and password, which is required to connect to the Internet;

2) Your ISP gave you software such as WinPOET or Enternet300 that you use to connect to the Internet; or

3) You have to double-click on a desktop icon other than your browser to get on the Internet.

1. User Name

This space is provided to type in your user name that was assigned by your ISP.

2. Password

Type in your password and re-type it into the "Retype Password" box to confirm it.

3. Service Name

A service name is rarely required by an ISP. If you are not sure if your ISP requires a service name, leave this blank.

4. MTU

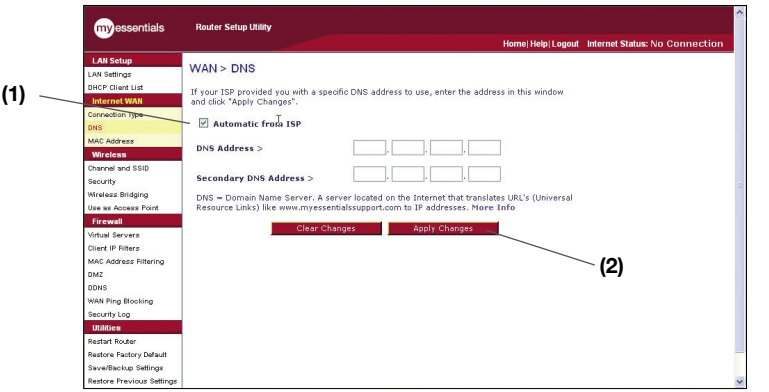
The MTU setting should never be changed unless your ISP gives you a specific MTU setting. Making changes to the MTU setting can cause problems with your Internet connection including disconnection from the Internet, slow Internet access, and problems with Internet applications working properly.

5. Maximum Idle Time

The "Maximum Idle Time" feature is used to automatically disconnect the Router from your ISP when there is no activity for a specified period of time. For instance, placing a check mark next to this option and entering "5" into the minute field will cause the Router to disconnect from the Internet after five minutes of no Internet activity. This option should be used if you pay for your Internet service by the minute.

Setting Custom Domain Name Server (DNS) Settings

A “Domain Name Server” is a server located on the Internet that translates Universal Resource Locators (URLs) like “www.MyEssentialssupport.com” into IP addresses. Many Internet Service Providers (ISPs) do not require you to enter this information into the Router. The “Automatic from ISP” box **(1)** should be checked if your ISP did not give you a specific DNS address. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is dynamic or PPPoE, it is likely that you do not have to enter a DNS address. Leave the “Automatic from ISP” box checked. To enter the DNS address settings, uncheck the “Automatic from ISP” box and enter your DNS entries in the spaces provided. Click “Apply Changes” **(2)** to save the settings.



Configuring your WAN Media Access Controller (MAC) Address

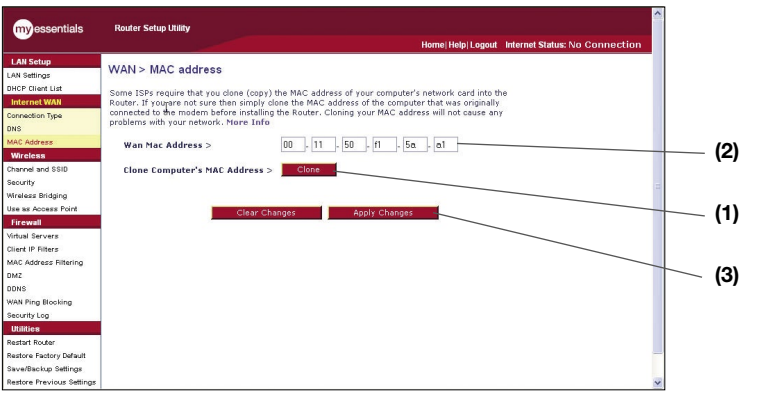
All network components including cards, adapters, and routers, have a unique "serial number" called a MAC address. Your Internet Service Provider may record the MAC address of your computer's adapter and only let that particular computer connect to the Internet service. When you install the Router, its own MAC address will be "seen" by the ISP and may cause the connection not to work. MyEssentials has provided the ability to clone (copy) the MAC address of the computer into the Router. This MAC address, in turn, will be seen by the ISP's system as the original MAC address and will allow the connection to work. If you are not sure whether your ISP needs to see the original MAC address, simply clone the MAC address of the computer that was originally connected to the modem. Cloning the address will not cause any problems with your network.

Cloning your MAC Address

To clone your MAC address, make sure that you are using the computer that was ORIGINALLY CONNECTED to your modem before the Router was installed. Click the “Clone” button **(1)**. Click “Apply Changes” **(3)**. Your MAC address is now cloned to the Router.

Entering a Specific MAC Address

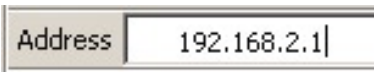
In certain circumstances you may need a specific WAN MAC address. You can manually enter one in the “MAC Address” page. Type in a MAC address in the spaces provided **(2)** and click “Apply Changes” **(3)** to save the changes. The Router’s WAN MAC address will now be changed to the MAC address you specified.



Using the Web-Based Advanced User Interface

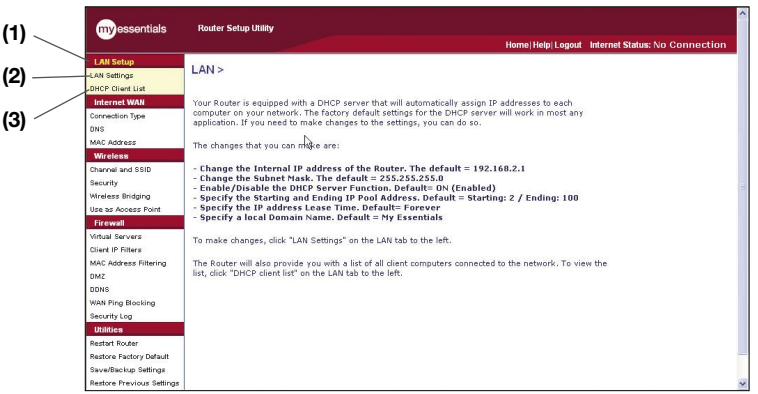
Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www"), then press the "Enter" key.

You will see the Router's home page in your browser window.



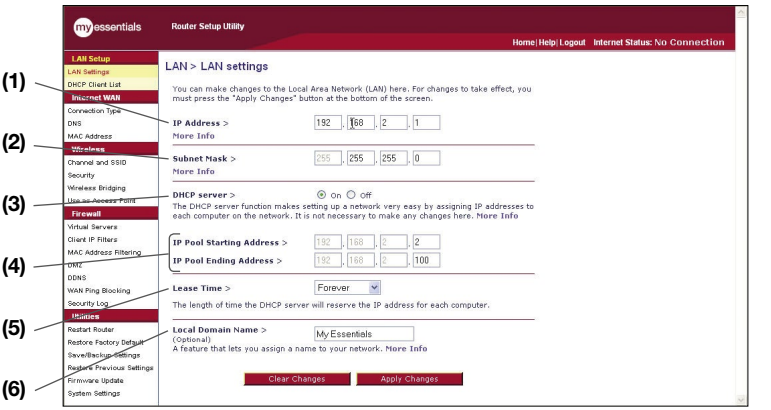
Viewing the LAN Settings

Clicking on the header of the "LAN Setup" tab **(1)** will take you its header page. A quick description of the functions can be found here. To view the settings or make changes to any of the LAN settings, click on "LAN Settings" **(2)**, or to view the list of connected computers, click on "DHCP Client List" **(3)**.


(1)
(2)
(3)
myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
LAN >
Your Router is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work in most any application. If you need to make changes to the settings, you can do so.
The changes that you can make are:
- Change the Internal IP address of the Router. The default = 192.168.2.1
- Change the Subnet Mask. The default = 255.255.255.0
- Enable/Disable the DHCP Server Function. Default= ON (Enabled)
- Specify the Starting and Ending IP Pool Address. Default = Starting: 2 / Ending: 100
- Specify the IP address Lease Time. Default= Forever
- Specify a local Domain Name. Default = My Essentials
To make changes, click "LAN Settings" on the LAN tab to the left.
The Router will also provide you with a list of all client computers connected to the network. To view the list, click "DHCP client list" on the LAN tab to the left.

Changing LAN Settings

All settings for the internal LAN setup of the Router can be viewed and changed here.


(1)
(2)
(3)
(4)
(5)
(6)
myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings
LAN > LAN settings
You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the "Apply Changes" button at the bottom of the screen.
IP Address > 192 . 168 . 2 . 1
More Info
Subnet Mask > 255 . 255 . 255 . 0
More Info
DHCP server > On Off
The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network. It is not necessary to make any changes here. More Info
IP Pool Starting Address > 192 . 168 . 2 . 2
IP Pool Ending Address > 192 . 168 . 2 . 100
Lease Time > Forever
The length of time the DHCP server will reserve the IP address for each computer.
Local Domain Name > (Optional)
My Essentials
A feature that lets you assign a name to your network. More Info
Clear Changes
Apply Changes

1. IP Address

The “IP address” is the internal IP address of the Router. The default IP address is “192.168.2.1”. To access the Web-Based Advanced User Interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click “Apply Changes”. The IP address you choose should be a non-routable IP.

Examples of a non-routable IP are: 192.168.x.x (where x is anywhere between 0 and 255), and 10.x.x.x (where x is anything between 0 and 255).

2. Subnet Mask

There is no need to change the subnet mask. This is a unique, advanced feature of your MyEssentials Router. It is possible to change the subnet mask if necessary; however, do NOT make changes to the subnet mask unless you have a specific reason to do so. The default setting is “255.255.255.0”.

3. DHCP Server

The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network automatically. The default setting is “On”. The DHCP server can be turned OFF if necessary; however, in order to do so you must manually set a static IP address for each computer on your network. To turn off the DHCP server, select “Off” and click “Apply Changes”.

4. IP Pool

The range of IP addresses set aside for dynamic assignment to the computers on your network. The default is 2–100 (99 computers). If you want to change this number, you can do so by entering a new starting and ending IP address and clicking on “Apply Changes”. The DHCP server can assign 100 IP addresses automatically. This means that you cannot specify an IP address pool larger than 100 computers. For example, starting at 50 means you have to end at 150 or lower so as not to exceed the 100-client limit. The starting IP address must be lower in number than the ending IP address.

5. Lease Time

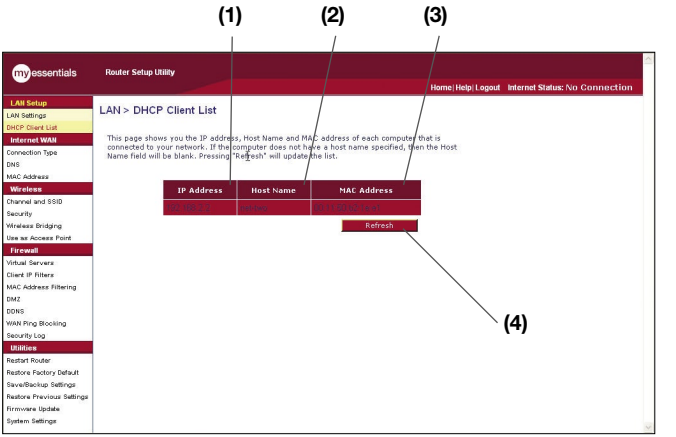
The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to “Forever”. The default setting is “Forever”, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular computer. Setting lease times for shorter intervals such as one day or one hour frees IP addresses after the specified period of time. This also means that a particular computer’s IP address may change over time. If you have set any of the other advanced features of the Router such as DMZ or client IP filters, these are dependent on the IP address. For this reason, you will not want the IP address to change.

6. Local Domain Name

The default setting is “MyEssentials”. You can set a local domain name (network name) for your network. There is no need to change this setting unless you have a specific advanced need to do so. You can name the network anything you want such as “MY NETWORK”.

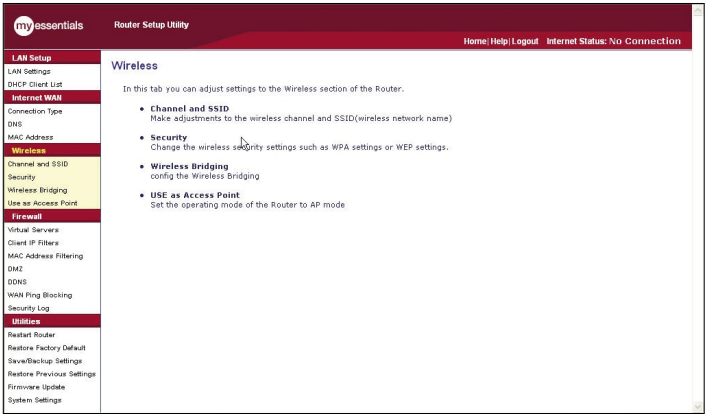
Viewing the DHCP Client List Page

You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address **(1)** of the computer, the host name **(2)** (if the computer has been assigned one), and the MAC address **(3)** of the computer's network interface card (NIC). Pressing the "Refresh" **(4)** button will update the list. If there have been any changes, the list will be updated.



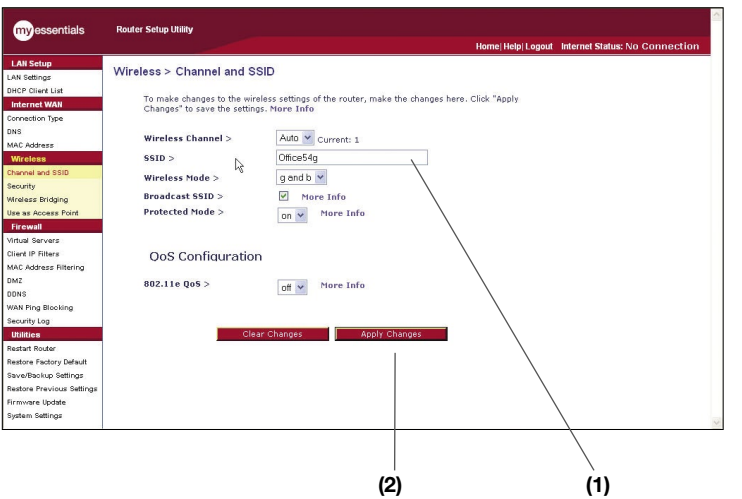
Configuring the Wireless Network Settings

Clicking on the header of the “Wireless” tab will take you to the “Wireless” header page. Under the “Wireless” tab, there are links that allow you to make changes to the wireless network settings.



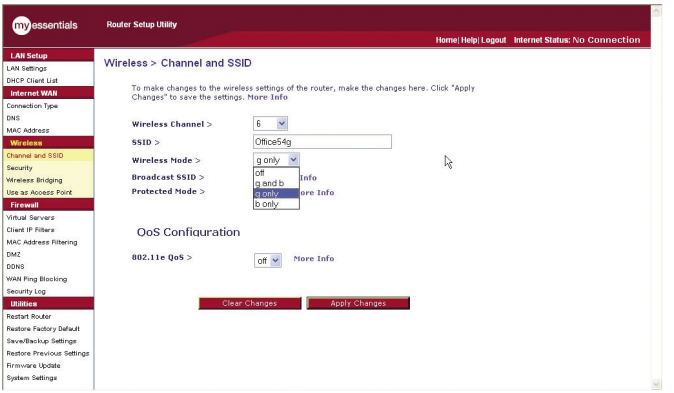
Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. The default SSID of the Router is “MyEssentials”. You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type in the SSID that you want to use in the “SSID” field **(1)** and click “Apply Changes” **(2)**. The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.



Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: “g and b”, “g only”, and “b only”. The different modes are explained below.



g and b Mode

In this mode, the Router is compatible with 802.11b and 802.11g wireless clients simultaneously. This is the factory default mode and ensures successful operation with all Wi-Fi-compatible devices. If you have a mix of 802.11b and 802.11g clients in your network, we recommend setting the Router to g and b mode. This setting should only be changed if you have a specific reason to do so.

g only Mode

g only mode works with 802.11g clients only. This mode is recommended only if you want to prevent 802.11b clients from accessing your network. To switch modes, select the desired mode from the “Wireless Mode” drop-down box. Then, click “Apply Changes”.

b only Mode

We recommend you DO NOT use this mode unless you have a very specific reason to do so. This mode exists only to solve unique problems that may occur with some 802.11b client adapters and is NOT necessary for interoperability of 802.11g and 802.11b standards.

When to use b only Mode

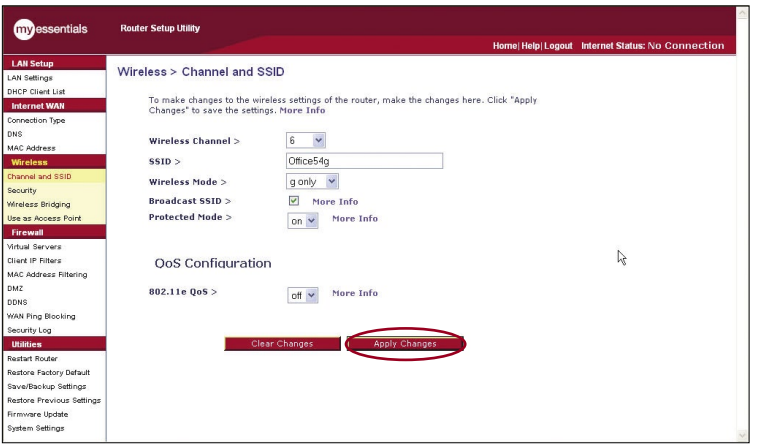
In some cases, older 802.11b clients may not be compatible with 802.11g wireless. These adapters tend to be of inferior design and may use older drivers or technology. Switching to this mode can solve problems that sometimes occur with these clients. If you suspect that you are using a client adapter that falls into this category of adapters, first check with the adapter vendor to see if there is a driver update. If there is no driver update available, switching to b only mode may fix your problem. **Please note that switching to b only mode will decrease 802.11g performance.**

QoS (Quality of Service) Configuration

QoS prioritizes important data on your network such as multimedia content and Voice over IP (VoIP) so it will not be interfered with by other data being sent over the network. Based on 802.11e, you can turn this feature on or off by selecting it from the drop-down menu and choosing the acknowledgement mode you want to use. If you plan to stream multimedia content or use VoIP on your network, we recommend that you enable the QoS feature.

Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States, there are 11 channels. In Australia, the United Kingdom, and most of Europe, there are 13 channels. In a small number of other countries, there are other channel requirements. Your Router is configured to operate on the proper channels for the country you reside in. The default channel is 11 (unless you are in a country that does not allow channel 11). The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks. For best performance, use a channel that is at least five channels away from the other wireless network. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the drop-down list. Click “Apply Changes”. The change is immediate.



Using the Broadcast SSID Feature

Note: This advanced feature should be employed by advanced users only.

For security, you can choose not to broadcast your network's SSID. Doing so will keep your network name hidden from computers that are scanning for the presence of wireless networks. To turn off the broadcast of the SSID, remove the check mark from the box next to "Broadcast SSID", and then click "Apply Changes". The change is immediate. Each computer now needs to be set to connect to your specific SSID; an SSID of "ANY" will no longer be accepted. Refer to the documentation of your wireless network adapter for information on making this change.

Protected Mode Switch

As part of the 802.11g specification, Protected mode ensures proper operation of 802.11g clients and access points when there is heavy 802.11b traffic in the operating environment. When Protected mode is ON, 802.11g scans for other wireless network traffic before it transmits data. Therefore, using this mode in environments with HEAVY 802.11b traffic or interference achieves best performance results. If you are in an environment with very little—or no—other wireless network traffic, your best performance will be achieved with Protected mode OFF.

Securing your Wi-Fi® Network

Here are a few different ways you can maximize the security of your wireless network and protect your data from prying eyes and ears. This section is intended for the home, home office, and small office user.

At the time of this User Manual's publication, there are four encryption methods available.

Name	64-Bit Wired Equivalent Privacy	128-Bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronym	64-bit WEP	128-bit WEP	WPA-TKIP/AES (or just WPA)	WPA2-AES (or just WPA2)
Security	Good	Better	Best	Best
Features	Static keys	Static keys	Dynamic key encryption and mutual authentication	Dynamic key encryption and mutual authentication
	Encryption keys based on RC4 algorithm (typically 40-bit keys)	More secure than 64-bit WEP using a key length of 104 bits plus 24 additional bits of system-generated data	TKIP (Temporal Key Integrity Protocol) added so that keys are rotated and encryption is strengthened	AES (Advanced Encryption Standard) does not cause any throughput loss

Wired Equivalent Privacy (WEP)

WEP is a common protocol that adds security to all Wi-Fi-compliant wireless products. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.

64-Bit WEP

64-bit WEP was first introduced with 64-bit encryption, which includes a key length of 40 bits plus 24 additional bits of system-generated data (64 bits total). Some hardware manufacturers refer to 64-bit as 40-bit encryption. Shortly after the technology was introduced, researchers found that 64-bit encryption was too easy to decode.

128-Bit WEP

As a result of 64-bit WEP's potential security weaknesses, a more secure method of 128-bit encryption was developed. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption.

Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All wireless networking products from MyEssentials support both 64-bit and 128-bit WEP.

Encryption Keys

After selecting either the 64-bit or 128-bit WEP encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another on your network and you will not be able to successfully communicate within your network.

You can enter your key by typing in the hex key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a key. A hex (hexadecimal) key is a combination of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key

The WEP passphrase is NOT the same as a WEP key. Your Router uses this passphrase to generate your WEP keys, but different hardware manufacturers might have different methods on generating the keys. If you have multiple vendors' equipment in your network, the easiest thing to do is to use the hex WEP key from your Router and enter it manually into the hex WEP key table in your Router's configuration screen.

Wi-Fi Protected Access (WPA)

WPA is a new Wi-Fi standard that was designed to improve upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support WPA. These updates will be found on the wireless vendor's website. There are three types of WPA security: WPA-PSK (no server), WPA (with radius server), and WPA2.

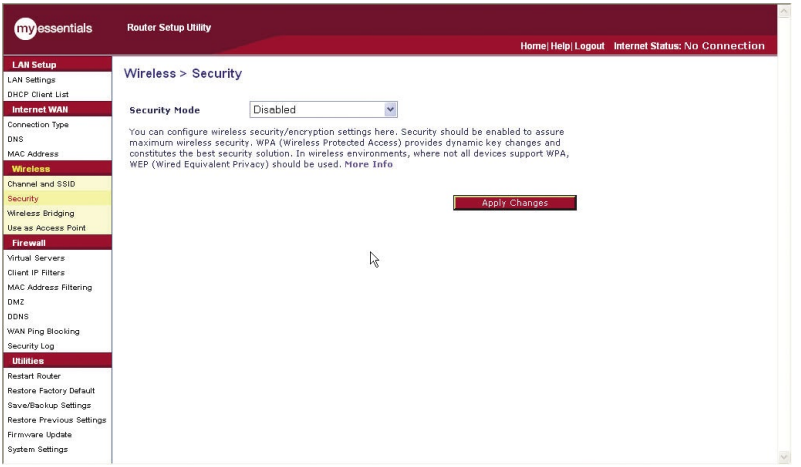
WPA-PSK (no server) uses what is known as a pre-shared key as the network key. A network key is basically a password that is between eight and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA (with radius server) is a system where a radius server distributes the network key to the clients automatically. This is typically found in a business environment.

WPA2 requires Advanced Encryption Standard (AES) for encryption of data, which offers much greater security than WPA. WPA uses both Temporal Key Integrity Protocol (TKIP) and (AES) for encryption.

Sharing the Same Network Keys

Most Wi-Fi products ship with security turned off. So once you have your network working, you need to activate WEP or WPA and make sure your wireless networking devices are sharing the same network key.



Using a Hexadecimal Key

A hexadecimal key is a combination of numbers and letters from A–F and 0–9. 64-bit keys are five two-digit numbers. 128-bit keys are 13 two-digit numbers.

For instance:

AF 0F 4B C3 D4 = 64-bit key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key

In the boxes below, make up your key by writing in two characters between A–F and 0–9 in each box. You will use this key to program the encryption settings on your Router and your wireless computers.

Note to Mac users: Original Apple® AirPort® products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

WEP Setup

64-Bit WEP Encryption

1. Select “64-bit WEP” from the “Security” menu’s “Security Mode”.

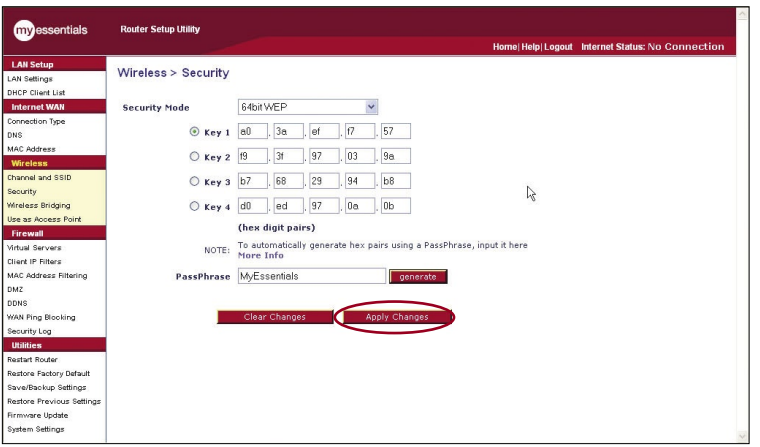
2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually, or you can put a check mark in “Passphrase”, then type in your passphrase. Click “Generate” to generate four different hex keys.

A hex (hexadecimal) key is a combination of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key

3. Click “Apply Changes” to save the setting.



WARNING: If you are configuring the Wireless G Router from a computer with a wireless client, you will need to ensure that security is turned ON for this wireless client. If this is not done, your client will lose its wireless connection.

128-Bit WEP Encryption

Note to Mac users: The passphrase option will not operate with Apple AirPort. To configure encryption for your Mac computer, set the encryption using the manual method described in the next section.

1. Select “128-bit WEP” from the “Security” menu’s “Security Mode”.

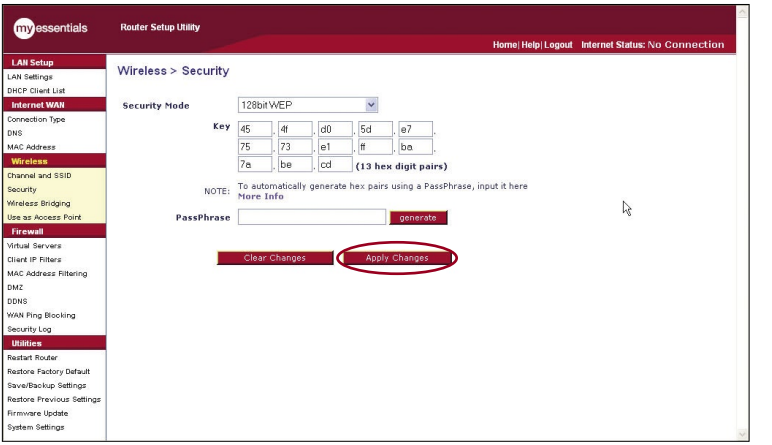
2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually, or you can put a check mark in “Passphrase”, then type in your passphrase. Click “Generate” to generate the hex keys.

A hex (hexadecimal) key is a combination of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key

3. Click “Apply Changes” to save the setting.



WARNING: If you are configuring the Wireless G Router from a computer with a wireless client, you will need to ensure that security is turned ON for this wireless client. If this is not done, your client will lose its wireless connection.

Changing the Wireless Security Settings

Your Router is equipped with WPA (Wi-Fi Protected Access), the latest wireless security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled. To enable security, you must first determine which standard you want to use. To access the security settings, click "Security" on the "Wireless" tab.

WPA Setup

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this User Manual's publication, a security patch download is available, for free, from Microsoft®. This patch works only with the Windows XP operating system. You must also download the latest driver for your Wireless G Notebook Network Card from the MyEssentials support site. Other operating systems are not supported at this time. Microsoft's patch supports only devices with WPA-enabled drivers such as MyEssentials 802.11g products.

WPA uses a so-called pre-shared key as the security key. A pre-shared key is a password that is between eight and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment.

WPA2 is the second generation of WPA, offering a more advanced encryption technique over WPA.

Setting WPA/WPA2

1. Select "WPA/WPA2-Personal (PSK)" from the "Security Mode" drop-down box.

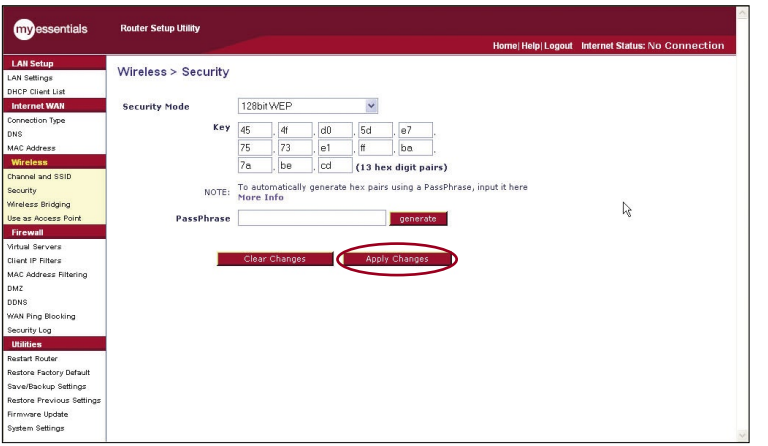
2. Select "WPA-PSK" for just WPA authentication, or "WPA2-PSK" for just WPA2 authentication, or you may select "WPA-PSK + WPA2-PSK" for WPA and WPA2 as the authentication type.

3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. This pre-shared key will allow users full access to your network including shared files and printers.

4. Click "Apply Changes" to finish. You must now set all clients to match these settings depending on the type of access you want them to have.

Guest Access (Optional)

The guest pre-shared key allows guest users an Internet-only access to restrict them from entering your network and having access to files on your PCs. Enter your pre-shared key for guest access. This can be from eight to 63 characters and can be letters, numbers, or symbols. Click "Apply Changes" to finish.



Setting up WPA for Wireless Desktop and Wireless Notebook Cards that are NOT MyEssentials

If you do NOT have a MyEssentials WPA Wireless Desktop or Wireless Notebook Card and it is not equipped with WPA-enabled software, a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access" is available for free download.

Please Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time.

Important: You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

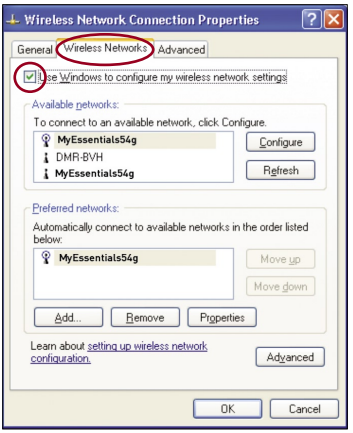
Setting up Windows XP Wireless Network Utility to use WPA-PSK

In order to use WPA-PSK, ensure you are using the Windows Wireless Network Utility by doing the following:

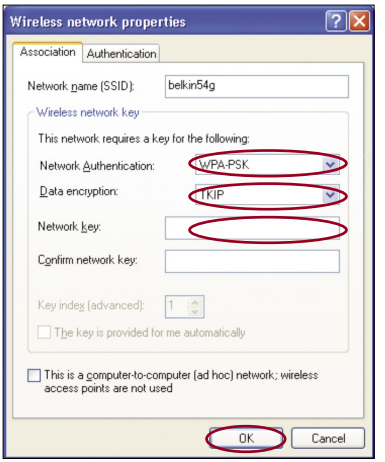
1. Under Windows XP, click “Start > Control Panel > Network Connections”.

2. Right-click on “Wireless Network Connection Properties” and select “Properties”.

3. Clicking on the “Wireless Networks” tab will display the following screen. Ensure the “Use Windows to configure my wireless network settings” box is checked.



4. Under the “Wireless Networks” tab, click the “Configure” button and you will see the following screen.



5. For a home or small business user, select “WPA-PSK” under “Network Authentication”.

Note: Select “WPA” if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Please consult your network administrator for further information.

6. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the Router that you set up.

7. Type in your encryption key in the “Network key” box.

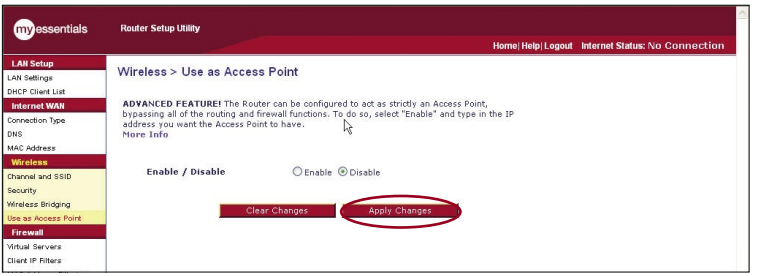
Important: Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.

8. Click “OK” to apply settings.

Using the Access Point Mode

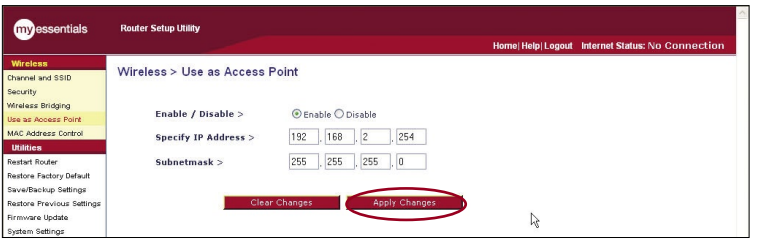
Note: This advanced feature should be employed by advanced users only. The Router can be configured to work as a wireless network access point. Using this mode will defeat the NAT IP sharing feature and DHCP server. In Access Point (AP) mode, the Router will need to be configured with an IP address that is in the same subnet as the rest of the network that you will bridge to. The default IP address is 192.168.2.254 and subnet mask is 255.255.255.0. These can be customized for your need.

1. Enable the AP mode my selecting “Enable” in the “Use as Access Point only” page. When you select this option, you will be able to change the IP settings.



2. Set your IP settings to match your network. Click “Apply Changes”.
3. Connect a cable from the “Modem” port on the Router to your existing network.

The Router is now acting as an access point. To access the Router’s Web-Based Advanced User Interface again, type the IP address you specified into your browser’s navigation bar. You can set the encryption settings, MAC address filtering, SSID, and channel normally.

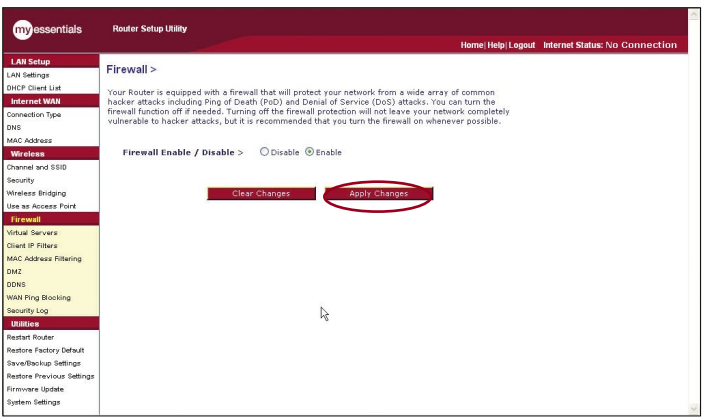


Configuring the Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

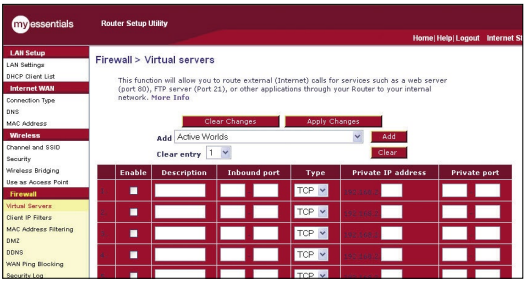
- IP Spoofing
- SYN flood
- Land Attack
- UDP flooding
- Ping of Death (PoD)
- Tear Drop Attack
- Denial of Service (DoS)
- ICMP defect
- IP with zero length
- RIP defect
- Smurf Attack
- Fragment flooding
- TCP Null Scan

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be “Stealth”, meaning that for all intents and purposes, they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.


myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings
Firewall >
Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.
Firewall Enable / Disable > Disable Enable
Clear Changes
Apply Changes

Configuring Internal Forwarding Settings

The “Virtual Servers” function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, computers outside your network (over the Internet) cannot get to them because they cannot be “seen.” You will need to contact the application vendor to find out which port settings you need.

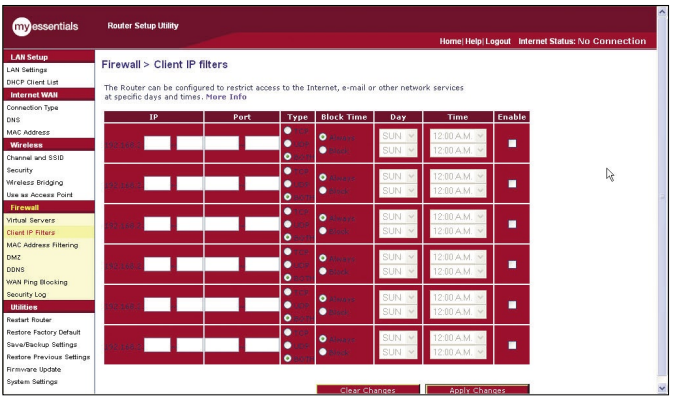


Entering Settings into the Virtual Server

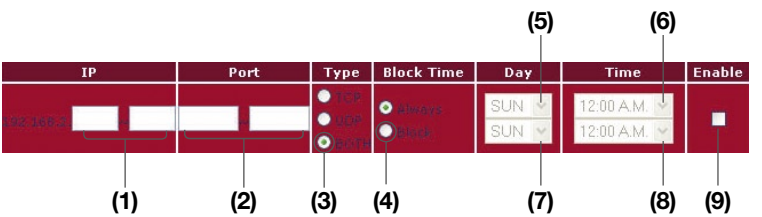
To enter settings, enter the IP address in the space provided for the internal (server) machine, and the port(s) required to pass. Then select the port type (TCP or UDP), check the “Enable” box, and click “Apply Changes”. Each inbound port entry has two fields with five characters maximum per field that allows a start and end port range, e.g. [xxxxx]-[xxxxx]. For each entry, you can enter a single port value by filling in the two fields with the same value (e.g. [7500]-[7500]) or a wide range of ports (e.g. [7500]-[9000]). If you need multiple single port values or a combination of ranges and a single value, you must use multiple entries up to the maximum of 20 entries (e.g. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Setting Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

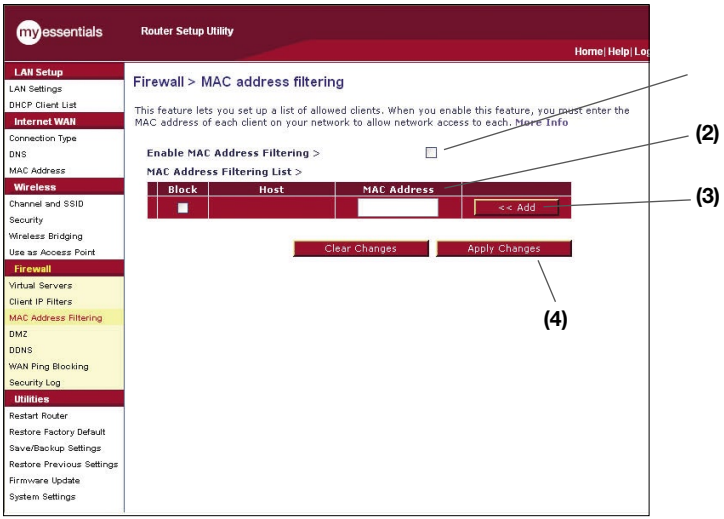


To restrict Internet access to a single computer for example, enter the IP address of the computer you wish to restrict access to in the IP fields **(1)**. Next, enter “80” in both the port fields **(2)**. Select “Both” **(3)**. Select “Block” **(4)**. You can also select “Always” to block access all of the time. Select the day to start on top **(5)**, the time to start on top **(6)**, the day to end on the bottom **(7)**, and the time to stop **(8)** on the bottom. Select “Enable” **(9)**. Click “Apply Changes”. The computer at the IP address you specified will now be blocked from Internet access at the times you specified. Note: Be sure you have selected the correct time zone under “Utilities> System Settings> Time Zone”.



Setting MAC Address Filtering

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) on your network to allow network access to each.

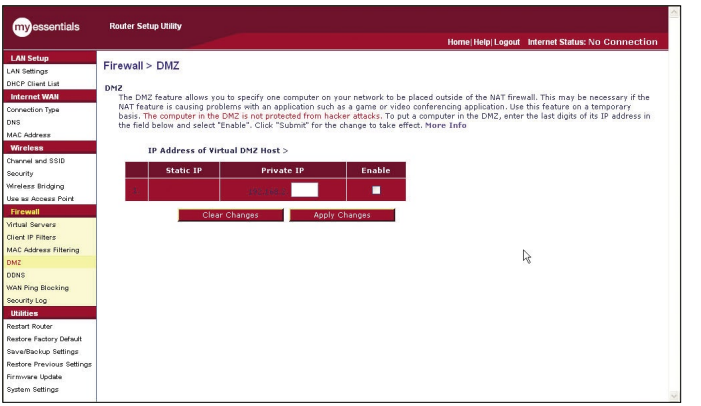


To enable this feature, select “MAC Address Filtering” and click “Enable MAC Address Filtering” **(1)**. Next, enter the MAC address of each computer on your network by clicking in the space provided **(2)** and entering the MAC address of the computer you want to add to the list. Click “Add” **(3)**, then “Apply Changes” **(4)** to save the settings. You can have a MAC-address-filtering list of up to 32 computers.

Note: You will not be able to delete the MAC address of the computer you are using to access the Router’s administrative functions (the computer you are using now).

Enabling the Demilitarized Zone (DMZ)

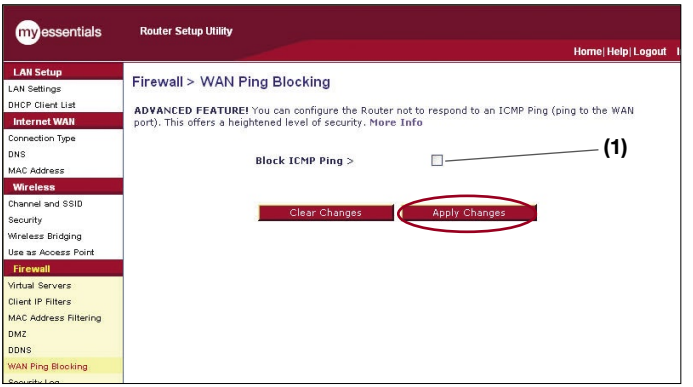
The DMZ feature allows you to specify one computer on your network to be placed outside of the firewall. This may be necessary if the firewall is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is NOT protected from hacker attacks. Note: If your ISP subscription provides you with additional public (WAN) IP addresses, additional computers can be placed outside the firewall provided each computer uses a different public (WAN) IP.


myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings
Firewall > DMZ
DMZ
The DMZ feature allows you to specify one computer on your network to be placed outside of the NAT firewall. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks. To put a computer in the DMZ, enter the last digits of its IP address in the field below and select "Enable". Click "Submit" for the change to take effect. More Info
IP Address of Virtual DMZ Host >
Static IP
Private IP
Enable
Clear Changes
Apply Changes

To put a computer in the DMZ, enter the last digits of its IP address in the IP field and select “Enable”. Click “Apply Changes” for the change to take effect.

WAN Ping Blocking

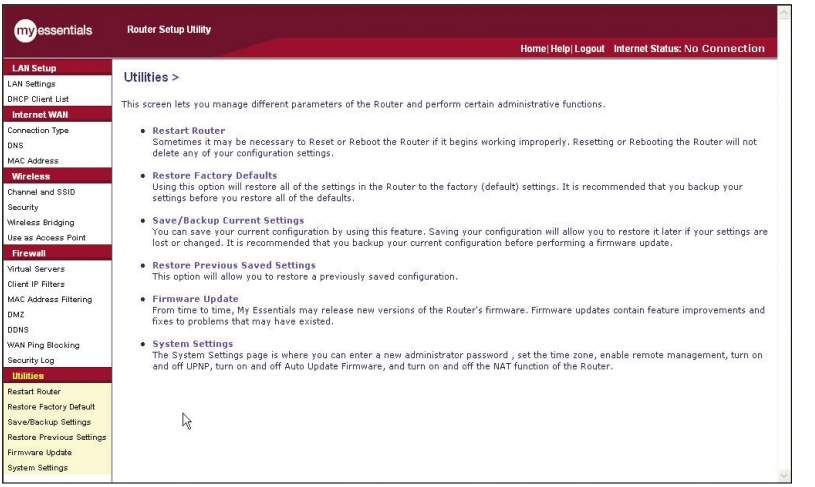
Computer hackers use what is known as “pinging” to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an ICMP ping from the outside. This heightens the level of security of your Router.



To turn off the ping response, select “Block ICMP Ping” **(1)** and click “Apply Changes”. The Router will not respond to an ICMP ping.

Utilities Tab

This screen lets you manage different parameters of the Router and perform certain administrative functions.


myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings
Utilities >
This screen lets you manage different parameters of the Router and perform certain administrative functions.
Restart Router
Sometimes it may be necessary to Reset or Reboot the Router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
Restore Factory Defaults
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
Save/Backup Current Settings
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
Restore Previous Saved Settings
This option will allow you to restore a previously saved configuration.
Firmware Update
From time to time, My Essentials may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
System Settings
The System Settings page is where you can enter a new administrator password , set the time zone, enable remote management, turn on and off UPNP, turn on and off Auto Update Firmware, and turn on and off the NAT function of the Router.

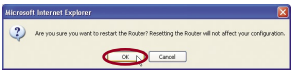
Restarting the Router

Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.

Restarting the Router to Restore Normal Operation

Utilities > Restart Router
Sometimes it may be necessary to Restart or Reboot the Router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.
Restart Router

1. Click the “Restart Router” button.


Microsoft Internet Explorer
Are you sure you want to restart the Router? Resetting the Router will not affect your configuration.
OK
Cancel

2. The following message will appear. Click “OK”.

Microsoft Internet Explorer
Allow up to 60 seconds for the Router to restart. Do not power down the Router before reset completes.
OK

3. The following message will appear. Restarting the Router can take up to 25 seconds. It is important not to turn off the power to the Router during the restart.

4. A 25-second countdown will appear on the screen. When the countdown reaches zero, the Router will be restarted. The Router’s home page should appear automatically. If not, type in the Router’s address (default = 192.168.2.1) into the navigation bar of your browser.

Restoring Factory Default Settings

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

Utilities > Restore Factory Defaults
Restore factory defaults
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.
Restore Defaults

1. Click the “Restore Defaults” button.

2. The following message will appear. Click “OK”.

3. The following message will appear. Restoring the defaults includes restarting the Router. It can take up to 25 seconds. It is important not to turn the power to the Router off during the restart.

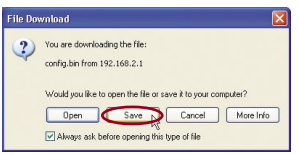
4. A 25-second countdown will appear on the screen. When the countdown reaches zero, the Router’s defaults will be restored. The Router’s home page should appear automatically. If it does not, type in the Router’s address (default = 192.168.2.1) into the navigation bar of your browser.

Saving a Current Configuration

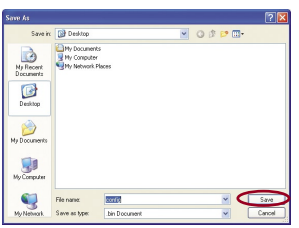
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.

1. Click “Save”. A window called “File Download” will open. Click “Save”.

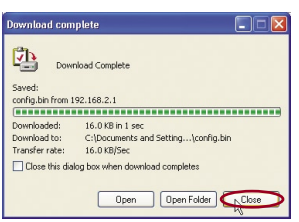
Utilities > Save/Backup current settings
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
Save


File Download
You are downloading the file:
config.bin from 192.168.2.1
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

2. A window will open that allows you to select the location where you want to save the configuration file. Select a location. You can name the file anything you want, or use the default name “Config”. Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file, click “Save”.



3. When the save is complete, you will see the following window. Click “Close”.

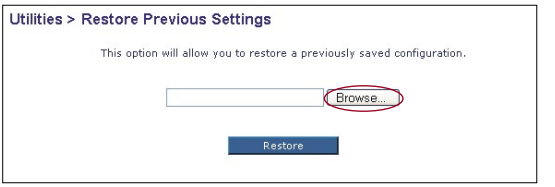


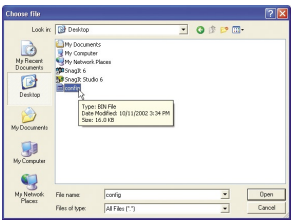
The configuration is now saved.

Restoring a Previous Configuration

This option will allow you to restore a previously saved configuration.

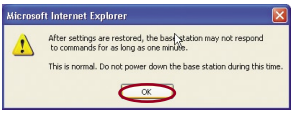
1. Click “Browse”. A window will open that allows you to select the location of the configuration file. All configuration files end with a “.bin”. Locate the configuration file you want to restore and double-click on it.


Utilities > Restore Previous Settings
This option will allow you to restore a previously saved configuration.
Browse...
Restore



2. You will be asked if you want to continue. Click “OK”.

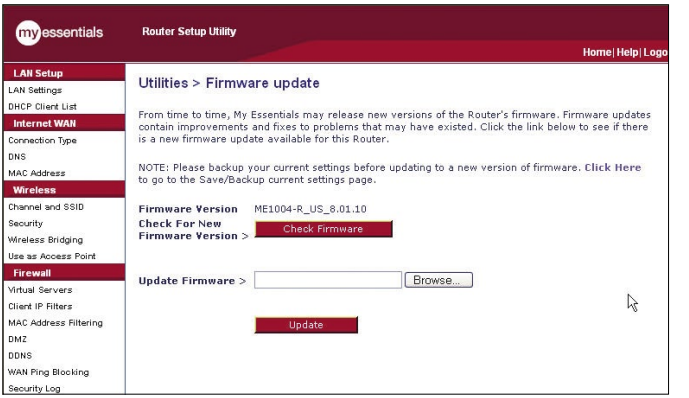
3. A reminder window will appear. It will take up to 35 seconds for the configuration restoration to complete. Click “OK”.


Microsoft Internet Explorer
After settings are restored, the base station may not respond to commands for as long as one minute.
This is normal. Do not power down the base station during this time.
OK

4. A 35-second countdown will appear on the screen. When the countdown reaches zero, the Router’s configuration will be restored. The Router’s home page should appear automatically. If not, type in the Router’s address (default = 192.168.2.1) into the navigation bar of your browser.

Updating the Firmware

From time to time, MyEssentials may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may exist. When MyEssentials releases new firmware, you can download the firmware from the MyEssentials update website and update your Router's firmware to the latest version.


myessentials
Router Setup Utility
Home | Help | Logo
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities > Firmware update
From time to time, My Essentials may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed. Click the link below to see if there is a new firmware update available for this Router.
NOTE: Please backup your current settings before updating to a new version of firmware. Click Here to go to the Save/Backup current settings page.
Firmware Version
ME1004-R_US_8.01.10
Check For New Firmware Version >
Check Firmware
Update Firmware >
Browse...
Update

Changing System Settings

The "System Settings" page is where you can enter a new administrator password, set the time zone, enable remote management, and turn on and off the NAT function of the Router.

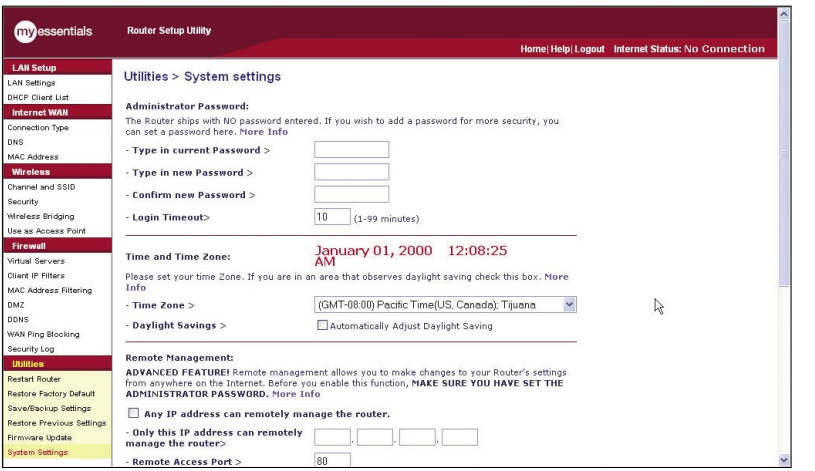
Setting or Changing the Administrator Password

The Router ships with NO password entered. If you wish to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log into the Router in the future. It is also recommended that you set a password if you plan to use the remote management feature of your Router.

Changing the Login Time-Out Setting

The login time-out option allows you to set the period of time that you can be logged into the Router's Web-Based Advanced User Interface. The timer starts when there has been no activity. For example, you have made some changes in the Web-Based Advanced User Interface, then left your computer alone without clicking "Logout". Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes.

Note: Only one computer can be logged into the Router's Web-Based Advanced User Interface at one time.

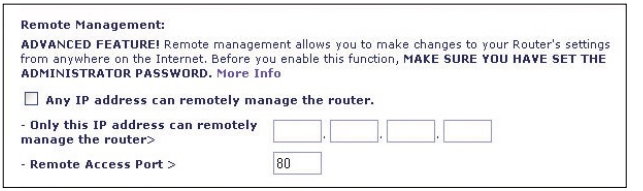

myessentials
Router Setup Utility
Home | Help | Logout Internet Status: No Connection
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wireless Bridging
Use as Access Point
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings
Utilities > System settings
Administrator Password:
The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. More Info
- Type in current Password >
- Type in new Password >
- Confirm new Password >
- Login Timeout>
10
(1-99 minutes)
Time and Time Zone:
January 01, 2000 12:08:25 AM
Please set your time Zone. If you are in an area that observes daylight saving check this box. More Info
- Time Zone >
(GMT-08:00) Pacific Time(US, Canada); Tijuana
- Daylight Savings >
Automatically Adjust Daylight Saving
Remote Management:
ADVANCED FEATURE! Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD. More Info
Any IP address can remotely manage the router.
- Only this IP address can remotely manage the router>
- Remote Access Port >
80

Setting the Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes daylight saving, then place a check mark in the box next to "Automatically Adjust Daylight Saving". The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

Enabling Remote Management

Before you enable this advanced feature of your MyEssentials Router, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD. Remote management allows you to make changes to your Router's settings from anywhere on the Internet. There are two methods of remotely managing the Router. The first is to allow access to the Router from anywhere on the Internet by selecting "Any IP address can remotely manage the Router". By typing in your WAN IP address from any computer on the Internet, you will be presented with a login screen where you need to type in the password of your Router. The second method is to allow a specific IP address only to remotely manage the Router. This is more secure, but less convenient. To use this method, enter the IP address you know you will be accessing the Router from in the space provided and select "Only this IP address can remotely manage the Router". Before you enable this function, it is STRONGLY RECOMMENDED that you set your administrator password. Leaving the password empty will potentially open your Router to intrusion.


Remote Management:
ADVANCED FEATURE! Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD. More Info
Any IP address can remotely manage the router.
- Only this IP address can remotely manage the router>
- Remote Access Port >
80

Enabling/Disabling Network Address Translation (NAT)

Note: This advanced feature should be modified by advanced users only.

NAT is the method by which the Router shares the single IP address assigned by your ISP with the other computers on your network and is enabled by default. NAT should only be disabled if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur. Turning off NAT will disable your firewall functions.

NAT Enabling:
ADVANCED FEATURE! Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. More Info
- NAT Enable / Disable >
Enable
Disable

Enabling/Disabling UPnP

UPnP (Universal Plug-and-Play) is yet another advanced feature offered by your MyEssentials Router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature. Simply select "Enable" in the "UPnP Enabling" section of the "Utilities" page. Click "Apply Changes" to save the change.

NAT Enabling:
ADVANCED FEATURE! Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. More Info
- NAT Enable / Disable >
Enable
Disable

Enabling/Disabling Auto Firmware Update

This innovation provides the Router with the built-in capability to automatically check for a new version of firmware and alert you that the new firmware is available. When you log into the Router's Web-Based Advanced User Interface, the Router will perform a check to see if new firmware is available. If so, you will be notified. You can choose to download the new version or ignore it. The Router ships with this feature enabled. If you want to disable it, select "Disable" and click "Apply Changes".

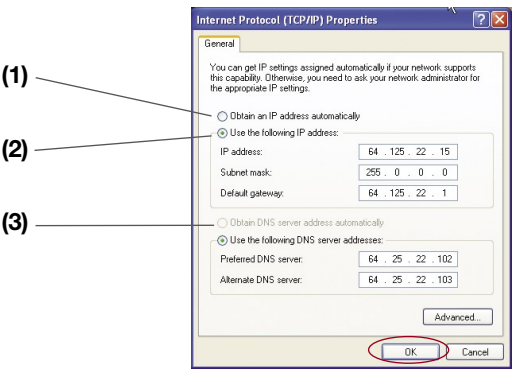
NAT Enabling:
ADVANCED FEATURE! Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. More Info
- NAT Enable / Disable >
Enable
Disable

Manually Configuring Network Settings

In order for your computer to properly communicate with your Router, you will need to change your PC's TCP/IP settings to DHCP.

Manually Configuring Network Adapters in Windows 2000, NT, or XP

1. Click "Start", "Settings", then "Control Panel".
2. Double-click on the "Network and dial-up connections" icon (Windows 2000) or the "Network" icon (Windows XP).
3. Right-click on the "Local Area Connection" associated with your network adapter and select "Properties" from the drop-down menu.
4. In the "Local Area Connection Properties" window, click "Internet Protocol (TCP/IP)" and click the "Properties" button. The following screen will appear:


(1)
(2)
(3)
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
64 . 125 . 22 . 15
Subnet mask:
255 . 0 . 0 . 0
Default gateway:
64 . 125 . 22 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
64 . 25 . 22 . 102
Alternate DNS server:
64 . 25 . 22 . 103
Advanced...
OK
Cancel

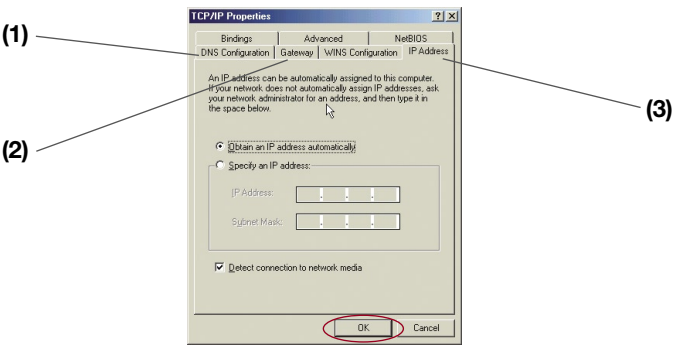
5. If "Use the following IP address" **(2)** is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.
6. If not already selected, select "Obtain an IP address automatically" **(1)** and "Obtain DNS server address automatically" **(3)**. Click "OK".

Your network adapter(s) are now configured for use with the Router.

Manually Configuring Network Adapters in Windows 98SE or Me

1. Right-click on “My Network Neighborhood” and select “Properties” from the drop-down menu.

2. Select “TCP/IP -> settings” for your installed network adapter. You will see the following window.



3. If “Specify an IP address” is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

4. Write in the IP address and subnet mask from the "IP Address" tab **(3)**.

5. Click the "Gateway" tab **(2)**. Write the gateway address down in the chart.

6. Click the "DNS Configuration" tab **(1)**. Write the DNS address(es) in the chart.

7. If not already selected, select "Obtain IP address automatically" in the "IP Address" tab. Click "OK".

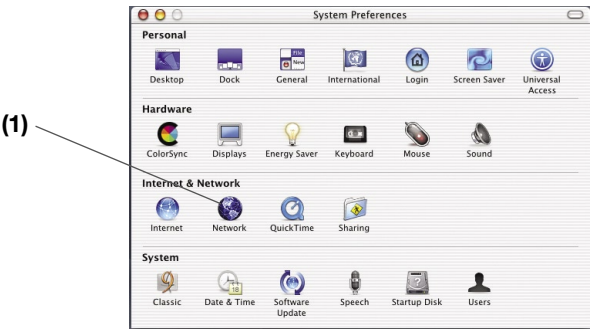
Restart the computer. When the computer restarts, your network adapter(s) are now configured for use with the Router.

Set up the computer that is connected to the DSL or cable modem FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

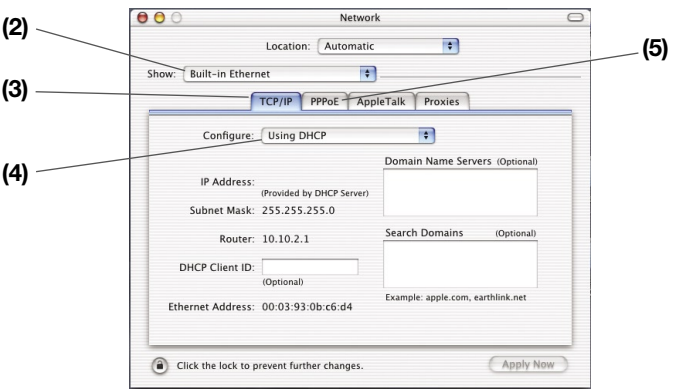
Manually Configuring Network Adapters in Mac OS X

1. Click on the “System Preferences” icon.

2. Select “Network” **(1)** from the “System Preferences” menu.

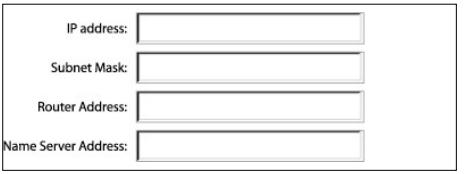


3. Select “Built-in Ethernet” **(2)** next to “Show” in the Network menu.



4. Select the "TCP/IP" tab **(3)**. Next to "Configure:" **(4)**, you should see "Manually" or "Using DHCP". If you do not, check the PPPoE tab **(5)** to make sure that "Connect using PPPoE" is NOT selected. If it is, you will need to configure your Router for a PPPoE connection type using your user name and password.

5. If "Manually" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.



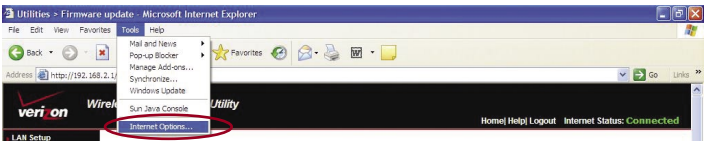
6. If not already selected, select "Using DHCP" next to "Configure:" **(4)**, then click "Apply Now".

Your network adapter(s) are now configured for use with the Router.

In most cases, you will not need to make any changes to your web browser's settings. If you are having trouble accessing the Internet or the Web-Based Advanced User Interface, then change your browser's settings to the recommended settings in this section.

Internet Explorer 4.0 or Higher

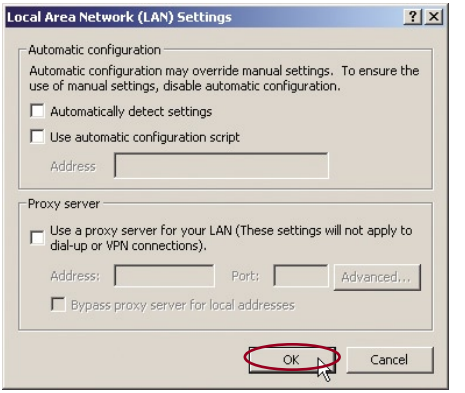
1. Start your web browser. Select "Tools" then "Internet Options".



2. In the "Internet Options" screen, there are three selections: "Never dial a connection", "Dial whenever a network connection is not present", and "Always dial my default connection". If you can make a selection, select "Never dial a connection". If you cannot make a selection, go to the next step.

3. Under the "Internet Options" screen, click on "Connections" and select "LAN Settings...".

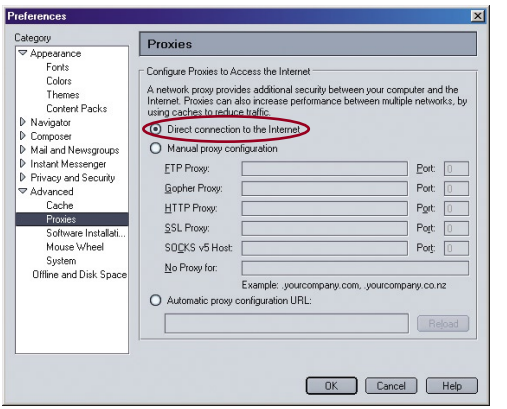
4. Make sure there are no check marks next to any of the displayed options: “Automatically detect settings”, “Use automatic configuration script”, and “Use a proxy server”. Click “OK”. Then click “OK” again in the “Internet Options” page.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced...
Bypass proxy server for local addresses
OK
Cancel

Netscape® Navigator® 4.0 or Higher

1. Start Netscape. Click on “Edit” then “Preferences”.

2. In the “Preferences” window, click on “Advanced” then select “Proxies”. In the “Proxies” window, select “Direct connection to the Internet”.



Problem:

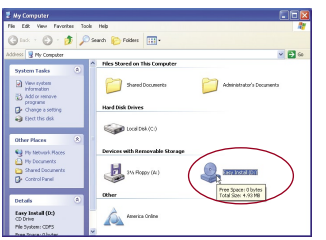
Installation CD does not automatically start.

Solution:

If the CD-ROM does not start the Quick Installation Software automatically, it could be that the computer is running other applications that are interfering with the CD drive.

1. If the Quick Installation Software screen does not appear within 15–20 seconds, open up your CD-ROM drive by double-clicking on the “My Computer” icon that is located on your desktop.

2. Next, double-click on the CD-ROM drive that the Quick Installation Software CD has been placed in to start the installation.



3. The Quick Installation Software should start within a few seconds. If, instead, a window appears showing the files on the CD, double-click on the icon labeled “EasyInstall.exe”.

4. If the Quick Installation Software still does not start, reference the section titled “Manually Configuring Network Settings” (page 75 of this User Manual) for an alternate setup method.

Problem:

The Quick Installation Software cannot find my Router.

Solution:

If the Quick Installation Software is not able to find the Router during the installation process, please check the following items:

1. If the Quick Installation Software is not able to find the Router during the installation process, there may be third-party firewall software installed on the computer attempting to access the Internet. Examples of third-party firewall software are ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, and Norton Personal Firewall.

   If you do have firewall software installed on your computer, please make sure that you properly configure it. You can determine if the firewall software is preventing Internet access by temporarily turning it off. If, while the firewall is disabled, Internet access works properly, you will need to change the firewall settings to function properly when it is turned on.

   Please refer to the instructions provided by the publisher of your firewall software for instructions on configuring the firewall to allow Internet access.

2. Unplug power to the Router for 10 seconds, and then plug the power back into the Router. Ensure that the Router's Power light is on; it should be solid green. If not, check to make sure that the AC adapter is correctly connected to the Router and plugged into a wall outlet.

3. Ensure that you have a cable (use the cable included with the Router) connected between (1) the network (Ethernet) port on the back of the computer and (2) one of the LAN ports, labeled "1" through "4", on the back of the Router.

   Note: The computer should NOT be connected to the port labeled "Internet/WAN" on the back of the Router.

4. Try shutting down and restarting your computer, then rerunning the Quick Installation Software.

   If the Quick Installation Software is still unable to find the Router, reference the section titled "Manually Configuring Network Settings" for installation steps.

Problem:

The Quick Installation Software cannot connect my Router to the Internet.

Solution:

If the Quick Installation Software is not able to connect the Router to the Internet, please check the following items:

1. Use the troubleshooting suggestions within the Quick Installation Software. If the troubleshooting screen does not open automatically, click on the “Troubleshoot” button in the lower, right-hand corner of the Quick Installation Software window.
2. If your ISP requires a user name and password, make sure that you have typed in your user name and password correctly. Some user names require that the ISP’s domain be at the end of the name. Example: “myname@myisp.com”. The “@myisp.com” part of the user name may need to be typed as well as your user name.

   If you continue to have no Internet connection, reference the section titled “Manually Configuring Network Settings” (page 75 of this User Manual) for an alternate setup method.

Problem:

- The Quick Installation Software completed installation, but my web browser doesn't work.
- I am unable to connect to the Internet. The Router's "WAN" light is off and the "Connected" light is blinking.

Solution:

If you cannot connect to the Internet, the "WAN" light is off, and the "Connected" light is blinking, the problem may be that your modem and Router are not connected properly.

1. Make sure the network cable between the modem and the Router is connected. We strongly recommend using the cable that was supplied with your DSL or cable modem for this purpose. The cable should be connected at one end to the Router's "Internet/WAN" port, and at the other end to the network port on your modem.

2. Unplug the DSL or cable modem from its power source for three minutes. After three minutes, plug the modem back into its power source. This may force the modem to properly recognize the Router.

3 Unplug the power to your Router, wait 10 seconds, and then reconnect the power. This will cause the Router to reattempt communication with the modem.

If the "WAN" light on the Router is not lit after completing these steps, please contact MyEssentials Technical Support at 866-761-4608.

4. Try shutting down and restarting your computer.

Problem:

- The Quick Installation Software completed installation, but my web browser doesn't work.
- I am unable to connect to the Internet. The Router's "WAN" light is on and the "Connected" light is blinking.

Solution:

If you cannot connect to the Internet, the "WAN" light is on, and the "Connected" light is blinking, the problem may be that your connection type may not match the ISP's connection.

- If you have a "static IP address" connection, your ISP must assign you the IP address, subnet mask, and gateway address. Please refer to the section entitled "Alternate Setup Method" for details on changing this setting.
- If you have a "PPPoE" connection, your ISP will assign you a user name and password and sometimes a service name. Make sure the Router connection type is configured to PPPoE and the settings are entered properly. Please refer to the section entitled "Alternate Setup Method" for details on changing this setting.
- You may need to configure your Router to meet the specific requirements of your ISP.

  If you are still unable to access the Internet after verifying these settings, please contact MyEssentials Technical Support at 866-761-4608.

Problem:

- The Quick Installation Software completed, but my web browser doesn't work.
- I am unable to connect to the Internet. The "WAN" light on my Router is blinking and the "Connected" light is solid.

Solution:

If the "WAN" light is blinking and the "Connected" light is solid, but you are unable to access the Internet, there may be third-party firewall software installed on the computer attempting to access the Internet. Examples of third-party firewall software are ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, and Norton Personal Firewall.

If you do have firewall software installed on your computer, please make sure that you properly configure it. You can determine if the firewall software is preventing Internet access by temporarily turning it off. If, while the firewall is disabled and Internet access works properly, you will need to change the firewall settings to function properly when it is turned on.

Please refer to the instructions provided by the publisher of your firewall software for instructions on configuring the firewall to allow Internet access.

If you are still unable to access the Internet after disabling any firewall software, please contact MyEssentials Technical Support at 866-761-4608.

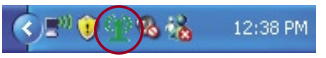
Problem:

I can't connect to the Internet wirelessly.

Solution:

If you are unable to connect to the Internet from a wireless computer, please do the following:

1. Look at the lights on your Router. Your MyEssentials Router's lights should be as follows:
   - The "Power" light should be on.
   - The "Connected" light should be on and not blinking.
   - The "WAN" light should be either on or blinking.
2. Open your wireless utility software by clicking on the icon in the system tray at the bottom, right-hand corner of the screen. If you are also using a Wireless Card or Adapter from MyEssentials with this Router, the tray icon should look like this (the icon may be red or green):



3. The exact window that opens will vary depending on the model of wireless card you have; however, any of the utilities should have a list of "Available Networks"—those wireless networks to which it can connect.

Does the name of your wireless network appear in the results?

Yes, my network name is listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, but my network name is listed".

No, my network name is not listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, and my network name is not listed".

Problem:

I can't connect to the Internet wirelessly, but my network name is listed.

Solution:

If the name of your network is listed in the "Available Networks" list, please follow the steps below to connect wirelessly:

1. Click on the correct network name in the "Available Networks" list.
2. If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see the section entitled "Securing your Wi-Fi Network" in this User Manual.
3. Within a few seconds, the tray icon in the lower, left-hand corner of your screen should turn green, indicating a successful connection to the network.

Problem:

I can't connect to the Internet wirelessly, and my network name is not listed.

Solution:

If the correct network name is not listed under "Available Networks" in the wireless configuration utility, please attempt the following troubleshooting steps:

1. Temporarily move your computer, if possible, five to 10 feet away from the Router. Close the wireless configuration utility, and reopen it. If the correct network name now appears under "Available Networks", you may have a range or interference problem. Please see the suggestions discussed in the section titled "Placement of your Router for Optimal Performance" in this User Manual.
2. Using a computer that is connected to the Router through a network cable (as opposed to wirelessly), ensure that "Broadcast SSID" is enabled. This setting is found on the Router's wireless "Channel and SSID" configuration page.

   If you are still unable to access the Internet after completing these steps, please contact MyEssentials Technical Support 866-761-4608.

Problem:

My wireless network performance is inconsistent.

Data transfer is sometimes slow.

Signal strength is poor.

I am having difficulty establishing and/or maintaining a Virtual Private Network (VPN) connection.

Solution:

Wireless technology is radio-based, which means connectivity and the throughput performance between devices decreases when the distance between devices increases. Other factors that will cause signal degradation (metal is generally the worst culprit) are obstructions such as walls and metal appliances. As a result, the typical indoor range of your wireless devices will be between 100 to 200 feet. Note also that connection speed may decrease as you move farther away from the Router.

In order to determine if wireless issues are related to range, we suggest temporarily moving the computer, if possible, five to 10 feet away from the Router.

Changing the Wireless Channel - Depending on local wireless traffic and interference, switching the wireless channel of your network can improve performance and reliability. The default channel the Router is shipped with is channel 11. You may choose from several other channels depending on your region (see the section titled “Changing the Wireless Channel” on page 42 for instructions on how to choose other channels).

Limiting the Wireless Transmit Rate - Limiting the wireless transmit rate can help improve the maximum wireless range and connection stability. Most wireless cards have the ability to limit the transmission rate. To change this property, go to the Windows Control Panel, open “Network Connections” and double-click on your wireless card’s connection. In the “Properties” dialog, select the “Configure” button on the “General” tab (Windows 98 users will have to select the wireless card in the list box and then click “Properties”), then choose the “Advanced” tab and select the rate property. Wireless client cards are usually set to automatically adjust the wireless transmit rate for you, but doing so can cause periodic disconnects when the wireless signal is too weak; as a rule, slower transmission rates are more stable.

Experiment with different connection rates until you find the best one for your environment; note that all available transmission rates should be acceptable for browsing the Internet. For more assistance, see your wireless card’s user manual.

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on the Router.

Solution:

1. Log into your Wireless Router.

   Open your web browser and type in the IP address of the Wireless Router (the Router's default is 192.168.2.1). Log into your Router by clicking on the "Login" button in the top, right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the password field blank and click "Submit".

   Click the "Wireless" tab on the left of your screen. Select the "Encryption" or "Security" tab to get to the security settings page.

2. Select "128-bit WEP" from the drop-down menu.

3. After selecting your WEP encryption mode, you can type in your hex WEP key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a WEP key from the passphrase. Click "Apply Changes" to finish. You must now set all of your clients to match these settings. A hex (hexadecimal) key is a combination of numbers and letters from A—F and 0—9. For 128-bit WEP, you need to enter 26 hex keys.

   For example:

   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key

4. Click "Apply Changes" to finish. Encryption in the Wireless Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

   WARNING: If you are configuring the Wireless Router from a computer with a wireless client, you will need to ensure that security is turned on for this wireless client. If this is not done, you will lose your wireless connection.

   Note to Mac users: Original Apple AirPort products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your Apple AirPort product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a client card from MyEssentials (Wireless Network Card or Adapter).

Solution:

The client card must use the same key as the Wireless G Router or access point. For instance, if your Wireless Router or access point uses the key 00112233445566778899AABBCC, then the client card must be set to the exact same key.

1. Double-click the "Signal Indicator" icon to bring up the "Wireless Networking Utility" screen. The "Advanced" button will allow you to view and configure more options of your client card.

2. Once the "Advanced" button is clicked, the Wireless Networking Utility (WNU) from MyEssentials will appear. The WNU will allow you to manage all the advanced features of the client card from MyEssentials.

3. Under the "Wireless Network Properties" tab, select a network name from the "Available Networks" list and click the "Properties" button.

4. Under "Data Encryption", select "WEP".

5. Ensure the box "The key is provided for me automatically" at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.

6. Type your WEP key in the "Network key" box.

   Important: A WEP key is a combination of numbers and letters from A—F and 0—9. For 128-bit WEP, you need to enter 26 keys. This network key needs to match the key you assign to your Wireless G Router or access point.

   For example:
   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key

7. Click "OK", and then "Apply" to save the settings.

If you are NOT using a wireless client card from MyEssentials, please consult the manufacturer's user manual for that wireless client card.

Problem:

Do MyEssentials products support WPA?

Solution:

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this publication, a security patch download is available, for free, from Microsoft. This patch works only with the Windows XP operating system.

Download the patch here:

http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as MyEssentials 802.11g products.

Download the latest driver at www.MyEssentialssupport.com for the following products:

ME1000-USB, ME1002-NB, ME1004-R

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Wireless Router from MyEssentials for a home network.

Solution:

1. From the "Security Mode" drop-down menu, select "WPA-PSK (no server)".

2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.

3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, symbols, or spaces. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".

4. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a client card from MyEssentials (Wireless Network Card or Adapter) for a home network.

Solution:

Clients must use the same key that the Wireless G Router or access point uses. For instance, if the key is “Smith Family Network Key” in the Wireless G Router or access point, the clients must also use that same key.

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Networking Utility” screen. The “Advanced” button will allow you to view and configure more options of your client card.

2. Once the “Advanced” button is clicked, the Wireless Networking Utility from MyEssentials (WNU) will appear. The WNU will allow you to manage all the advanced features of the client card from MyEssentials.

3. Under the “Wireless Network Properties” tab, select a network name from the “Available Networks” list and click the “Properties” button.

4. Under “Network Authentication”, select “WPA-PSK (no server)”.

5. Type your WPA key in the “Network key” box.

   Important: WPA-PSK is a combination of numbers and letters from A—Z and 0—9. For WPA-PSK, you can enter eight to 63 characters. This network key needs to match the key you assign to your Wireless G Router or access point.

6. Click “OK”, then “Apply” to save the settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a client card from MyEssentials (Wireless Network Card or Adapter) for a business.

Solution:

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Networking Utility” screen. The “Advanced” button will allow you to view and configure more options of your client card.
2. Once the “Advanced” button is clicked, the WNU will appear. This Utility will allow you to manage all the advanced features of the client card from MyEssentials.
3. Under the “Wireless Network Properties” tab, select a network name from the “Available Networks” list and click the “Properties” button.
4. Under “Network Authentication”, select “WPA”.
5. In the “Authentication” tab, select the settings that are indicated by your network administrator.
6. Click “OK”, then “Apply” to save the settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security and I am NOT using a client card from MyEssentials for a home network.

Solution:

If you are NOT using a Wireless Notebook Network Card from MyEssentials and it is not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download:

http://www.microsoft.com/downloads/search.aspx?displaylang=en

Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time. You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

Enabling WPA-PSK (no server)

1. In systems running Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-click on the “Wireless Networks” tab. The “Wireless Network Connection Properties” screen appears. Ensure the “Use Windows to configure my wireless network settings” box is checked.
3. Under the “Wireless Networks” tab, click the “Configure” button, and you will see the client card properties screen.
4. For a home or small business user, select “WPA-PSK” under “Network Administration”.
5. Select “TKIP” or “AES” under “Date Encryption”. This setting will have to be identical to the Wireless G Router or access point that you set up.
6. Type in your encryption key in the “Network key” box. Important: Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.
7. Click “OK” to apply settings.

FCC Statement

DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

We, MyEssentials, of 501 West Walnut Street, Compton, CA 90220, declare under our sole responsibility that the product,

ME1004-R

to which this declaration relates,
complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: Exposure to Radio Frequency Radiation.
The radiated output power of this device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized. When connecting an external antenna to the device, the antenna shall be placed in such a manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Federal Communications Commission Notice
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications to this device that are not expressly approved by MyEssentials may void the user's authority to operate the equipment.

MyEssentials 1-Year Limited Product Warranty

MyEssentials warrants this product against defects in materials and workmanship for one year. If a defect is discovered, MyEssentials will, at its option, repair or replace the product at no charge provided it is returned during the warranty period, with transportation charges prepaid, to the authorized MyEssentials dealer from whom you purchased the product. Proof of purchase may be required.

This warranty does not apply if the product has been damaged by accident, abuse, misuse, or misapplication; if the product has been modified without the written permission of MyEssentials; or if any MyEssentials serial number has been removed or defaced.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. MYESSENTIALS SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No MyEssentials dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

MYESSENTIALS IS NOT RESPONSIBLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO, LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE TO OR REPROGRAMMING OR REPRODUCING ANY PROGRAM OR DATA STORED IN, OR USED WITH, MYESSENTIALS PRODUCTS.

Some states do not allow the exclusion or limitation of incidental or consequential damages or exclusions of implied warranties, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

myessentials

Wireless G Router

www.MyEssentialssupport.com

MyEssentials Tech Support:
US: 1-866-761-4608

© 2006 Belkin Corporation. All rights reserved. All trade names are registered trademarks of respective manufacturers listed. Mac OS and AppleTalk are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Windows, NT, and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

P75284